L Number	Hits	Search Text	DB	Time stamp
1	2165	713/200.ccls.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 21:48
2	48	713/200.ccls. and "email" and "virus"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 21:49
3	22	713/200.ccls. and "email" and "virus" and "attachment"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 21:53
4	26	713/201.ccls. and "email" and "virus" and "attachment"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 21:55
5	1961	709/206.ccls.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 21:55
7	13	709/206.ccls. and receipt.ti.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 22:03
8	1412	709/206.ccls. and (email or e-mail)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 22:03
9	506	709/206.ccls. and (email or e-mail) and attachment$3	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 22:03
10	2	709/206.ccls. and (email or e-mail) and attachment$3 and "automatic reply"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 22:08
11	3	709/206.ccls. and (email or e-mail) and attachment$3 and "delivery receipt"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 22:12
12	79	(email or e-mail) and attachment$3 and "delivery receipt"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 22:12
13	0	(email or e-mail) and attachment$3 and "delivery receipt" and "automatic reply"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 22:12
14	5632	(email or e-mail) and attachment$3 and"automatic reply"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 22:12

15	12	(email or e-mail) and attachment$3 and "automatic reply"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 22:13
16	60	(email or e-mail) and "automatic reply"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 22:20
17	1961	709/206.ccls.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 22:20
19	3	709/206.ccls. and mail with receipt.ti.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 22:21
20	2	5138653.pn.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/18 22:21
21	38	5138653.URPN.	USPAT	2004/04/18 22:29
22	17	"benign virus"	USPAT	2004/04/18 22:31
23	1	"benign virus" and "email"	USPAT	2004/04/18 22:38
24	15	auto-reply	USPAT	2004/04/18 22:38
25	5	auto-reply and (e-mail or email)	USPAT	2004/04/18 22:42
26	0	"computer virus avoidance system"	USPAT	2004/04/18 22:42
27	0	"computer virus avoidance"	USPAT	2004/04/18 22:42
28	1	"virus avoidance"	USPAT	2004/04/18 22:42
29	44	"attachment" with reply$3	USPAT	2004/04/18 22:43
30	4067	"attachment" with repl$4	USPAT	2004/04/18 22:43
31	37	"attachment" with repl$4 and (email or e-mail)	USPAT	2004/04/18 22:48
32	7	(email or e-mail) with (automatic near repl$8)	USPAT	2004/04/18 22:51
33	1	5754857.pn.	USPAT	2004/04/18 22:52
34	4079	(email or e-mail) and receipt	USPAT	2004/04/18 22:52
35	506	(e-mail or email) with receipt	USPAT	2004/04/18 22:52
36	85	(e-mail or email) with receipt with (notification or delivery or auto)	USPAT	2004/04/18 22:53

US006618747B1

(12) **United States Patent**
Flynn et al.

(10) **Patent No.: US 6,618,747 B1**
(45) **Date of Patent: Sep. 9, 2003**

(54) **ELECTRONIC COMMUNICATION DELIVERY CONFIRMATION AND VERIFICATION SYSTEM**

(76) Inventors: **Francis H. Flynn**, 14 Wave Crest Dr., Islip, NY (US) 11751; **Jeffrey Foran**, 1127 Commonwealth Ave., Apt. 1, Allston, MA (US) 02134

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/448,365**

(22) Filed: **Nov. 23, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/109,934, filed on Nov. 25, 1998.

(51) **Int. Cl.**[7] **G06F 15/16**
(52) **U.S. Cl.** **709/206**; 709/203
(58) **Field of Search** 709/203, 206, 709/217; 345/744, 752; 379/93.24

(56) **References Cited**

U.S. PATENT DOCUMENTS

RE34,954	E	5/1995	Haber et al.	
5,426,594	A *	6/1995	Wright et al.	709/206
5,509,071	A	4/1996	Petrie, Jr. et al.	
5,675,733	A	10/1997	Williams	
5,748,738	A	5/1998	Bisbee et al.	
5,771,355	A *	6/1998	Kuzma	709/232
5,793,972	A *	8/1998	Shane	709/219
5,850,520	A	12/1998	Griebenow et al.	
5,903,723	A	5/1999	Beck et al.	
5,930,471	A *	7/1999	Milewski et al.	709/204
6,018,774	A	1/2000	Mayle et al.	
6,275,848	B1 *	8/2001	Arnold	709/206
6,332,164	B1 *	12/2001	Jain	709/235
6,385,655	B1 *	5/2002	Smith et al.	709/232
6,477,243	B1 *	11/2002	Choksi et al.	379/100.06

FOREIGN PATENT DOCUMENTS

WO WO 02/25508 A2 * 3/2002

OTHER PUBLICATIONS

Gralla, P., How the Intranets Work, Ziff-Davis Press, pp. xi & 122–125, 1996.*

Stallings, W., Data and Computer Communications, Prentice-Hall, pp. 728–730, 1997.*

Lowe, D., Client/Server Computing for Dummies, IDG Books Worldwide, pp. 125–128 and 136–137, 1995.*

Gralla, P., How the Internet Works, Special Edition, Ziff-Davis Press, pp. 76–86, 110–111 and 122–125.*

Microsoft Press Computer Dictionary, 3rd ed., Microsoft Press, pp. 34–35, 1997.*

Klensin et al; Request for Comments: RFC 1869 (Nov. 1995) available at http://www.gssnet.com/rfc/rfc1869.htm, pp. 1–11.

Freed; Request for Comments: RFC 2034 (Oct. 1996) available at http://www.gssnet.com/rfc/rfc2034.htm, pp. 1–5.

Mosher, Sue; Microsoft Exchange User's Handbook; Duke Press (1997); pp. 220, 285, 288.

Blue Mountain Arts. Frequently Asked Questions. www-.bluemountain.com/help/FAQ2.html, pp. 5–6 & 11.

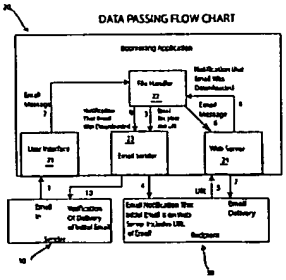
* cited by examiner

Primary Examiner—Andrew Caldwell
(74) *Attorney, Agent, or Firm*—Collard & Roe PC

(57) **ABSTRACT**

The present invention provides a system and a method for a user to verify receipt of an electronic communication such as an email message by an intended recipient. Instead of forwarding the email to the intended recipient(s), (e.g. as a normal SMTP server might,) the invention sends a notification message of a posted email to the intended recipient(s). The email and attachments are each saved at a unique call address on a server such as for example a web server. At least one unique address is provided for each of the intended recipients that points to the location of the contents of the original email. When attachments accompany the email, each attachment is also assigned an address that is unique for each intended recipient. The intended recipient is notified of the call addresses for collecting the email and attachments. When the recipient downloads or collects the email and attachments from their respective addresses, the invention detects information regarding the downloaded email and notifies the sender that the email was retrieved. This information may be stored in a back-end database for ease of access and management.

6 Claims, 2 Drawing Sheets



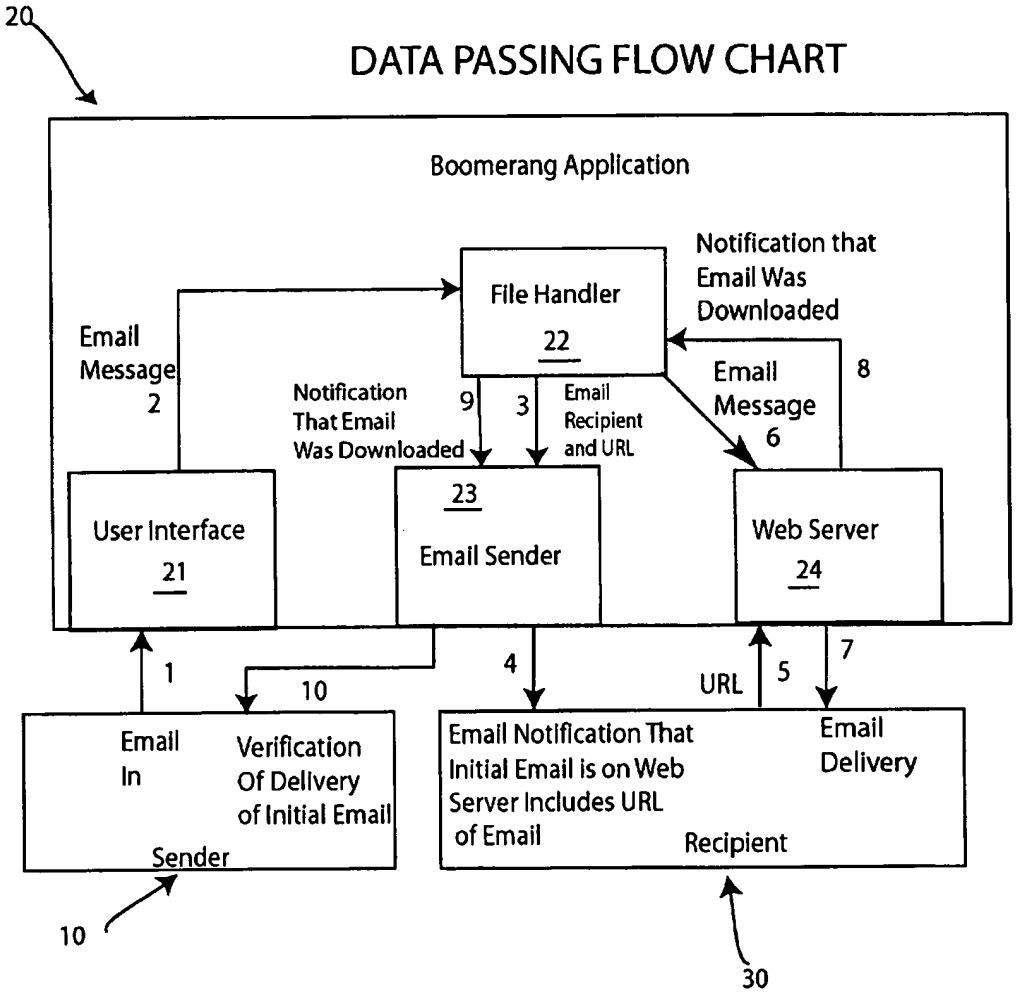
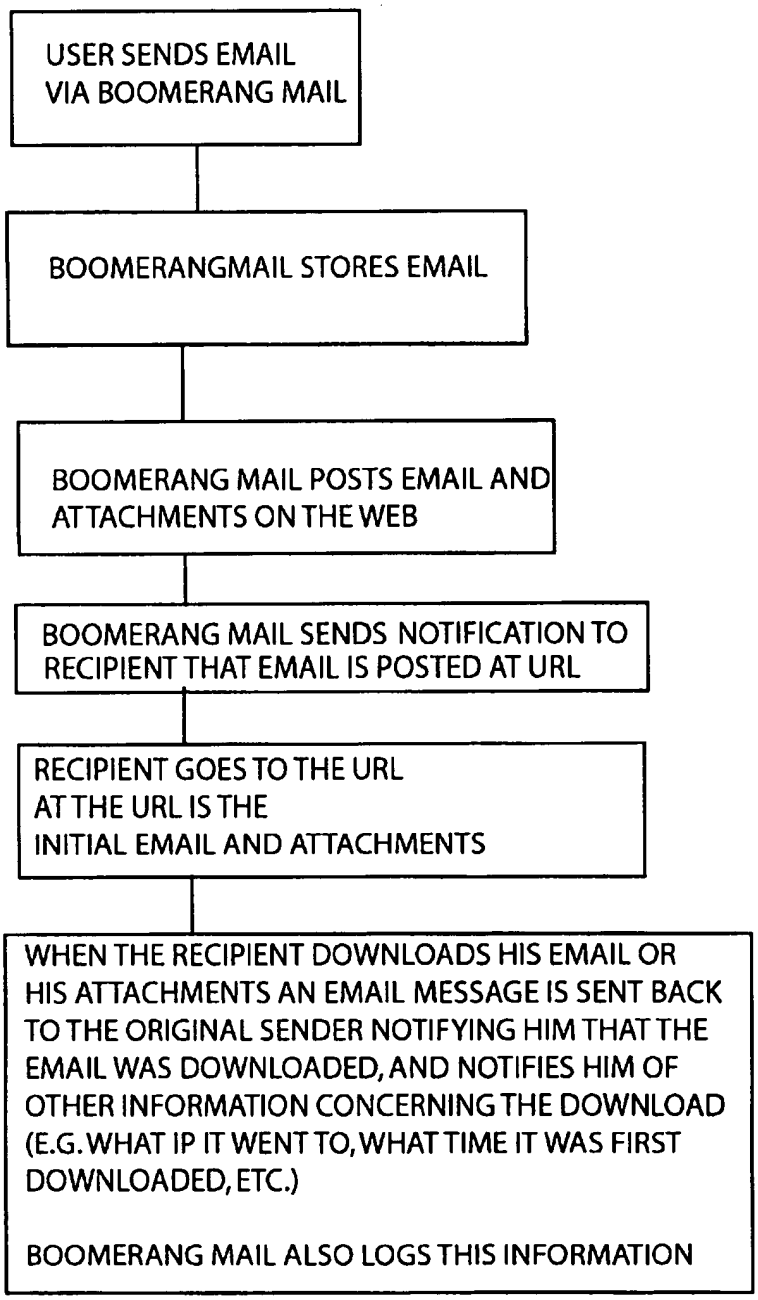

20
DATA PASSING FLOW CHART
Boomerang Application
File Handler
22
Notification that
Email Was
Downloaded
Email
Message
2
Notification
That Email
Was Downloaded
9
3
Email
Recipient
and URL
Email
Message
6
8
User Interface
21
23
Email Sender
Web Server
24
1
10
4
URL
5
7
Email
In
Verification
Of Delivery
of Initial Email
Sender
Email Notification That
Initial Email is on Web
Server Includes URL
of Email
Email
Delivery
Recipient
10
30

FIG. 1

FIG. 2

SEQUENCE OF STEPS TAKEN DURING BOOMERANG MAIL USE



ELECTRONIC COMMUNICATION DELIVERY CONFIRMATION AND VERIFICATION SYSTEM

This application claims the benefit of U.S. Provisional Patent Application 60/109,934 filed Nov. 25, 1998, entitled "An Electronic Communication Delivery Verification System", the content of which is incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

This invention relates generally to electronic communications and, more particularly, to a method by which a sender of an electronic communication can validate receipt of an electronic communication by an intended receiver.

BACKGROUND OF INVENTION

Electronic communication, such as for example e-mail, is a form of written data, a data-string, that is transported electronically such as on the Internet. Specific protocols governing certain aspects of the way one machine electronically passes information in the form of data-strings to another machine have been established to facilitate communication between different brands of machines running different software. Various protocols have been developed to standardize the methods by which data are transported from one computer to another computer such as on Local Area Networks (LAN), Wide Area Networks (WAN), and the Internet. This standardization was developed to allow computers and computer programs from differing commercial sources to be as compatible as possible.

The Internet Protocol (IP) that directs or routes a data-string from one computer to another is what is called a best efforts protocol, a method that involves a series of computer instructions that attempts to deliver a data-string to its intended location, but that does not guarantee its delivery. This means that the data-string can get lost or damaged before reaching the intended recipient. The Transmission Control Protocol (TCP) works in conjunction with IP in an attempt to ensure that data-string is sent error-free, complete, and in the proper sequence. However, it does not insure correct delivery. The Simple Mail Transfer Protocol (SMTP) provides for standardized error messages to be issued when a fault occurs in transmission. Standardized status codes (such as described in Kleinsin, et al; Network Working Group Request for Comments: 1869; STD: 10: Obsoletes: 1651; Category: Standards Track; November, 1995) provide information for generating error messages that indicate whether or not a computer in the net or network of computers used to pass the data-string has been unable to do so. Such an Error message is exemplified by:

"----The following addresses had delivery problems ----
<nosuchuser@dbc.mtview.ca.us>
(Mailbox "nosuchuser" does not exist)"

When delivery occurs a message such as "---Mail was successfully relayed to the following addresses---" may be provided. However, no information is provided by through the use of these protocols via the respective protocol server regarding whether the intended recipient has retrieved the email and/or the attachments.

Business people and others need to verify that an important transaction once sent has been received by the intended recipient. The main obstacle to widespread commercial use of electronic communications, such as for example email and email attachment, is the lack of the ability to verify that the email and/or attachment was received by the intended recipient. Email must be sent on unsecured pathways, pathways where the email can be mis-directed, lost, and/or altered. It is highly desirable to the sender to be able to verify that the intended recipient has received an important email. It is also desirable to the sender to know that the intended information in electronic message was received as written or sent.

SUMMARY OF INVENTION

The instant invention comprises a software application for use with a computer that is part of or has access to an electronic network including at least one other computer and a method for use of the software application that provides a sender of an electronic communication such as an email, a receipt for verification of delivery of the electronic communication by a recipient. The sender may use a conventional email program or the instant invention to compose the email. The email ("electronic mail") may have graphics and/or attachments, each of which is termed a data-string herein. Unlike a conventional email program, each data-string is directed to a unique electronic address, such as for example an IP (Internet Protocol) address or hostname, on a computer that is independent of the recipient's computer. Only a notification that an email or an email plus an attachment is awaiting retrieval is sent to the recipient and appears at their computer. The notification provides the recipient with the unique electronic retrieval location(s), such as a unique IP address for an email message or two unique email addresses for an email accompanied by an attachment, located on a mail server to which the recipient can direct their computer using software to retrieve the data-string(s). Each recipient is provided with a unique address to retrieve their email even when the recipient is merely receiving a copy of an email that has been broadcast to a number of recipients. In one embodiment, a computer having access to the Internet is used as the mail server. In an alternate embodiment, the mail server is located on a LAN (local area network) such as for example for use for infra-office email within a business. Upon retrieval of the data-string, the sender is notified electronically via email and information regarding the retrieval transaction is stored in a back-end database.

For example, when the data-string is sent via the Internet, the user who is the sender composes an email message and attaches any text or images as required. Once the message is composed and sent, the instant invention parses that data-string while determining the appropriate recipients. The parsed data-string is placed on the World Wide Web (also termed the Web or the Internet or the Net) by waiting until at least one appropriate data-string transfer and retrieval means, such as for example a HyperText Transport Protocol (http) call provides an available address at a port of a computer the instant invention is monitoring. More addresses will be needed to match data-string to address when, for example, a single email data-string is being communicated to a number of different recipients. There is exactly one unique address that will access the data-string for each specific recipient targeted to receive the data-string unless the data-string has more than one component such as a plurality of attachments. Concurrent with posting the sender's data-string on a computer connected to a network of computers such as the Web, the instant invention sends out a notice via email that the recipient has a posted data-string or email awaiting retrieval. This message is simply a notice of the availability of the electronic communication that provides an electronic address such as a Uniform Resource Locator (URL) pointer to where the email is posted on the Web. One URL points to a single location that

is uniquely assigned for each component of the data-string for each recipient using the instant invention. Alternatively, the posted email may have a URL that allows it to call for its accompanying attachment ie. the email and its accompanying documents may be electronically interlinked.

When the recipient of the email message links to a data-string via the URL pointer, the instant invention identifies the recipient by their unique IP address or hostname. As the recipient retrieves their posted email message and attachments, the instant invention notifies the sender that the posted electronic communication has been retrieved by a person at the IP address corresponding to that of the intended recipient. This notice includes the recipient's unique IP address or hostname and a time, date stamp indicative of when the posted electronic communication was retrieved. A copy of the posted electronic communication may also be included in the notice.

An embodiment of an inventive method for verifying receipt of an electronic communication at an intended electronic address is provided by the following example comprising the steps of:

1. Sending an electronic communication comprising a data-string.
2. Posting that data-string to a unique URL on a computer connected to the Web for each unique data-string.
3. Notifying the recipient at a recipient IP address via email that they have an electronic communication awaiting retrieval at a specified unique Web URL address.
4. Validating the retrieval of the sender's electronic communication by a recipient at an intended IP address by recognizing the recipient's IP address or hostname when they electronically request delivery of their electronic communication.
5. Notifying the sender when the IP address or hostname match the intended IP address or hostname that the electronic communication has been retrieved and optionally passing the validating information into a back-end database.

The invention has four distinct interfaces with users: two sender interfaces and two recipient interfaces. The first sender interface is an outgoing message interface that is implemented to communicate with any SMTP client having an outgoing server that is configurable to a given IP address or hostname. This interface is not limited to what is generally considered client type programs such as for example email programs such as Eudora®. The invention could interface at the first sender interface with any large server that delivers email using SMTP where the outgoing delivery IP address is capable of being configured. The first recipient interface is implemented to accommodate use with any system or application that handles delivery of electronic messages to a given recipient. This includes all POP clients, all Web-based email clients as well as any test-based email delivery and retrieval systems. The second part of the recipient interface is the data-string retrieval interface. This interface is implemented to communicate only via http (with any http browser in the embodiments described. However, the recipient interface can be implemented to accommodate any data-string retrieval mechanism. The second sender interface is the incoming interface that notifies the sender when the data-string is retrieved. In one embodiment, it is implemented as an email delivery notification and works with any system that handles delivery of email to a given recipient. This includes all POP clients, all Web based clients, as well as any text-based email retrieval systems.

In one embodiment, the instant invention communicates (also termed "interfaces") with electronic communications program, such as for example email programs Eudora®, First Class Client®, and Hot Mail®. It can be used for electronic communication on the Internet or an Intranet, within a Local Area Network (LAN) or a Wide Area Network (WAN) environment. The invention provides a plurality of fields for data in the back-end database. Full search, browse, edit, and contact management functions are included in order to provide complete access to the stored data. Remote access functions may be configured. Thus, verification, authentication, and ease of data management are provided. Advantageously, the flow of electronic communications such as email can be controlled and documented.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 provides a block diagram of the system and method by which an electronic communication in the form of data can be routed by a sender to a specific receiver and by which the sender can be notified of the receipt of the electronic communication by the specific receiver.

FIG. 2 provides a flow chart of the pathway and components used to transmit and verify an electronic communication.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The instant invention provides a system and method for confirmation of receipt of an electronic communication by an IP address or hostname accessible recipient ("the recipient"). The invention is a software application that allows the sender of an electronic communication to use the electronic communication program of their choice, such as for example an email program like Eudora®, to generate a specific data-string or message, send it to a specific recipient, and verify that the specific recipient received the data-string. Optionally, the application may provide a copy of the retrieved data-string so that the sender can determine if the data-string was received as sent, unaltered. Transmission of electronic information involves passing data in the form of a data-string from one computer to another through the use of computer programs that convert user instructions into instructions that a computer can understand. The data-string is then passed through electronic means, such as for example by telephone wires or cables, from one computer to another computer. These computers form a network of computers that is variously referenced to as a "Net" or "Web".

The invention has four distinct interfaces with users: two sender interfaces and two recipient interfaces. The first sender interface is an outgoing message interface that is implemented to communicate with any SMTP client having an outgoing server that is configurable to a given IP address or hostname. This interface is not limited to what is generally considered client type programs such as for example email programs such as Eudora®. The invention could interface at the first sender interface with any large server that delivers email using SMTP where the outgoing delivery IP address is capable of being configured. The first recipient interface is implemented to accommodate use with any system or application that handles delivery of electronic messages to a given recipient. This includes all POP clients, all Web-based email clients as well as any test-based email delivery and retrieval systems. The second part of the recipient interface is the data-string retrieval interface. This

interface is implemented to communicate only via http (with any http browser in the embodiments described. However, the recipient interface can be implemented to accommodate any data-string retrieval mechanism. The second sender interface is the incoming interface that notifies the sender when the data-string is retrieved. In one embodiment, it is implemented as an email delivery notification and works with any system that handles delivery of email to a given recipient. This includes all POP clients, all Web based clients, as well as any text-based email retrieval systems.

Referring now to FIG. **1** which illustrates a first embodiment of the instant invention, when an electronic communication sender is distanced from a recipient and the Internet is used to send the electronic communication, a sender illustrated by box "Sender" **10** enters information, such as for example an email message and an attachment to that email message, into a computer via the desired electronic communications program that has been loaded on that sender's machine. A message data-string is generated. This message data-string is then processed by the instant invention which has been loaded on the sender's machine as follows. The message data-string is parsed into an html-readable file and electronically sent via a user interface **21** to a file handler **22** where the message data-string is stored at a unique http call address assigned to each of the intended recipients. Assignment of the unique http call address(es) is determined by the instant invention which monitors a port for incoming TCP connections. If the electronic communication was an email that included an attachment, then a unique address is assigned to each of the parsed original email message and original attachment html-readable files. Concurrently upon receiving a file for storage, the file handler also generates a unique data-string for each stored file that is a notification message that is delivered to each unique recipient. This notification data-string informs each recipient that one unique message data-string has been stored for them at the indicated unique http call address. This notification data-string is sent via a Web Server **24** to the intended unique recipient, represented by box "recipient" **30**.

The notification data-string may have additional information added to it prior to its delivery to the recipient. For example, the electronic communication sender's name and/or email address may be added. Or, an advertisement may be added to the notification message data-string.

The notification message data-string is then sent to the recipient's Post Office Protocol (POP) server and is read by the recipient at the notified IP address or hostname address indicated by the notification message when they open their email application. If the recipient wishes to read the posted electronic communication, the recipient enters the unique http call address that has been sent in the notification message data-string and retrieves the unique message data-string from the Web Server **24**, if the recipient has entered the correct http call address. Both an email and its associated attachment(s) can be provided with unique call addresses or the email and its attachment(s) can be linked so that the entire communication is available using one call address. In a first embodiment for each stored message data-string retrieved, be it email or attachment, the Web server sends a notification of receipt message that informs the sender that the message data-string was retrieved by the recipient at the address receiving the notification of available email and http call address. This notification of receipt message is electronically transmitted to the sender at approximately the same time that the recipient is sent (retrieves) the stored message data-string. The notification of receipt message is sent via the file handler and the email sender to the IP or hostname address of the sender ("original sender") and includes information concerning the downloading of the message data-string by the recipient, such as for example, the time it was first downloaded (time and date stamp), the address to which it was sent at downloading, and other relevant information. A compressed copy of the message received by the recipient may also be provided to the sender.

If the original electronic communication comprises an email and an attachment, then in one embodiment, the recipient is notified that an electronic communication is located at http call address **1** (the email) and at http call address **2** (the attachment). The recipient retrieves the electronic communications at each address and notification of each separate retrieval is provided to the sender as described above. Alternatively, the notification message may contain a link to the address for the email and to the address for the attachment. Notification of receipt may then be sent as each data-string is retrieved or notification of receipt may be sent only once when all associated electronic communications have been retrieved.

FIG. **2** provides an embodiment of a method of confirming that an electronic communication was received by a recipient. This embodiment exemplifies electronic communication verification when using the Internet to transport the electronic communication. Referring now to FIG. **2**, a flowchart of the steps used to provide verification to a sender that receipt of a electronic communication by a recipient has occurred is provided. The sender installs the software, the inventive computer program for generating electronic mail receipts, on their computer and electronically moves through a set-up interface. The sender generates an electronic communication such as an email. The sender enters the email address of the intended recipient or recipients thus providing an addressed packet of information or a message data-string which includes the address of the intended recipient that is unique for each intended recipient. The message data-string is converted to html-readable language and passed to a file handler via a user interface. The message data-string is stored while the instant invention locates one unoccupied call address, such as for example an http call address, if the message data-string is going to only one recipient. Otherwise, the instant invention recognizes that a plurality of unique call address are required and establishes one unique call address for storage of each copy of the email sent to the plurality of intended recipients. In the simplest case where there is one recipient, the message data-string is then posted to this unique unoccupied call address which is on a Web server. Concurrently, a notice that the recipient has email from the sender on the Web server at the call address at which the message data-string is located is sent to the recipient's Post Office Protocol (POP) server, notifying the recipient that they have an electronic communication. The recipient requests the message data-string located at the provided unique call address and it is sent to the recipient, who downloads it, opening it. Upon downloading of the message data-string, the instant invention generates a notice of receipt that is forwarded to the original sender. The notice of receipt forwarded to the sender at the sender's POP server includes information concerning the collection of the email by the recipient such as for example the address to which the email was downloaded, the time it was downloaded, and optionally, a compressed copy of the original message. When the sender enters their POP server, they receive the notification of receipt by the recipient.

When attachments accompany an email, each of the attachments and the email itself is provided with a unique

call address. Each is collected separately by the intended recipient. The intended recipient may be notified of each separately or the intended recipient may be directed to the email call address which then provides the recipient with the unique call addresses of each of the attachments.

Notification of receipt of the email and attachments can be achieved in a variety of ways and may vary depending upon the number of recipients and the number of attachments sent. Notification can be sent as each unique recipient accesses each unique call address. Or, notification may be sent to the sender when the recipient has collected the email and all of its associated attachments. Or, where a plurality of recipients have been sent the same email, the sender may be notified only after all the recipients have retrieved their copies of the email. Preferably, in the notification of receipt, a copy of the electronic message as received by the recipient is included. This message may then be compared with the message sent to verify that the message was not garbled during transmission. Other options will be apparent to those skilled in the art.

The instant invention also may be inactivated without having to remove the software application off the computer hard disc. The instant software application is provided with the following switches: Override, Always On, and Switch. Override allows the user to substantially turn off the software application thus deactivating notification of receipt. "Always On" allows the user to send electronic communication which provides notification of receipt whenever the electronic communication is accessed. Switch provides a subroutine that reads the electronic communication before its is sent by the sender to determine if a receipt is being requested.

Modifications and variations can be made to the disclosed embodiments without departing from the subject and spirit of the invention as defined in the following claims. Such modifications and variations, as included within the scope of these claims, are meant to be considered part of the invention as described.

What is claimed is:

1. A method for verifying receipt by an intended recipient of an electronic communication generated by a sender comprising the following steps:

a) sending an electronic communication comprising a data-string having an electronic address for the intended recipient;

b) posting said data-string having said electronic address to a unique call address;

c) providing the intended recipient with said unique call address at said electronic address;

d) receiving at said call address a request, having said electronic address for the intended recipient therewith, to access said data string;

e) comparing said electronic address in said request with said electronic address provided in said data-string and proceeding with accessing said data string when said electronic address in said request matches said electronic address in said data-string;

f) sending an electronic notification consisting of data, said data comprising said call address and said electronic address of the intended recipient to the sender when said electronic communication is accessed by the intended recipient.

2. The method as in claim 1, further comprising the step of posting said data in a back end database.

3. A method for verifying receipt by an intended recipient of an electronic communication generated by a sender comprising the following steps:

a) sending an electronic communication comprising a data-string having an electronic address for the intended recipient;

b) sending an attachment to said electronic communication to an additional electronic address for the intended recipient;

c) posting said data-string having said electronic address to a unique call address;

d) posting said attachment having said additional electronic address to an additional unique call address;

e) providing the intended recipient with said unique call address at said electronic address;

f) receiving at said call address a request, having said electronic address for the intended recipient therewith, to access said data-string;

g) comparing said electronic address in said request with said electronic address provided in said data-string and proceeding with accessing said data string when said electronic address in said request matches said electronic address in said data-string; and

h) sending an electronic notification consisting of data, said data comprising said call address and said electronic address of the intended recipient to the sender when said electronic communication is accessed by the intended recipient.

4. The method as in claim 3, further comprising the step of posting said data in a back end database.

5. A device for verifying receipt by an intended recipient of an electronic communication generated by a sender comprising the following steps:

a) means for sending an electronic communication comprising a data-string having an electronic address for the intended recipient;

b) means for posting said data-string having said electronic address to a unique call address;

c) means for providing the intended recipient with said unique call address at said electronic address;

d) means for receiving at said call address a request, having said electronic address for the intended recipient therewith, to access said data string;

e) means for comparing said electronic address in said request with said electronic address provided in said datastring and proceeding with accessing said data string when said electronic address in said request matches said electronic address in said datastring; and

f) means for sending an electronic notification consisting of data, said data comprising said call address and said electronic address of the intended recipient to the sender when said electronic communication is accessed by the intended recipient.

6. A device for verifying receipt by an intended recipient of an electronic communication generated by a sender comprising the following steps:

a) means for sending an electronic communication comprising a data-string having an electronic address for the intended recipient;

b) means for sending an attachment to said electronic communication to an additional electronic address for the intended recipient;

c) means for posting said data-string having said electronic address to a unique call address;

d) means for posting said attachment having said additional electronic address to an additional unique call address;

e) means for providing the intended recipient with said unique call address at said electronic address;

f) means for receiving at said call address a request, having said electronic address for the intended recipient therewith, to access said data-string;

g) means for comparing said electronic address in said request with said electronic address provided in said datastring and proceeding with accessing said data string when said electronic address in said request matches said electronic address in said datastring; and

h) means for sending an electronic notification consisting of data, said data comprising said call address and said electronic address of the intended recipient to the sender when said electronic communication is accessed by the intended recipient.

* * * * *

US006687740B1

(12) **United States Patent**
Gough et al.

(10) **Patent No.: US 6,687,740 B1**
(45) **Date of Patent: Feb. 3, 2004**

(54) **SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR PREVENTING THE PROLIFERATION OF UNWANTED ELECTRONIC MESSAGES**

(75) Inventors: **Michael L. Gough**, Ben Lomond, CA (US); **James J. Gough**, Ben Lomond, CA (US)

(73) Assignee: **Neostar, Inc.**, Ben Lomond, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/401,028**

(22) Filed: **Sep. 21, 1999**

(51) **Int. Cl.**[7] **G06F 15/16**
(52) **U.S. Cl.** **709/206**; 709/202; 709/201; 709/203; 709/217; 709/218
(58) **Field of Search** 7409/201–203, 7409/205–207, 217–218

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,297,143	A	3/1994	Fridrich et al.
5,396,588	A	3/1995	Froessl
5,428,784	A	6/1995	Cahill, Jr.
5,513,126	A	4/1996	Harkins et al.
5,634,005	A	5/1997	Matsuo
5,659,729	A	8/1997	Nielsen
5,694,616	A	12/1997	Johnson et al.
5,724,521	A	3/1998	Dedrick
5,740,252	A	4/1998	Minor et al.
5,740,374	A	4/1998	Raffali-Schreinemachers
5,774,170	A	6/1998	Hite et al.
5,774,534	A	6/1998	Mayer
5,781,901	A	7/1998	Kuzma
5,790,789	A	8/1998	Suarez
5,793,972	A	8/1998	Shane
5,806,043	A	9/1998	Toader
5,809,242	A	9/1998	Shaw et al.
5,815,830	A	9/1998	Anthony
5,818,447	A	10/1998	Wolf et al.
5,826,023	A	10/1998	Hall et al.
5,826,062	A	10/1998	Fake, Jr. et al.

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

EP	0 340 039 B1	9/1999
EP	0 816 0990 A2	9/1999
JP	7-325827	9/1999
JP	10-171727	9/1999

OTHER PUBLICATIONS

The Internet article, "Death to Spam, A Guide to Dealing with Unwanted E–Mail" (herein after Death to Spam) obtained from the World Wide Web Address http://www.mindworkshop.com/alchemy/nospam.html on Sep. 21, 1999.

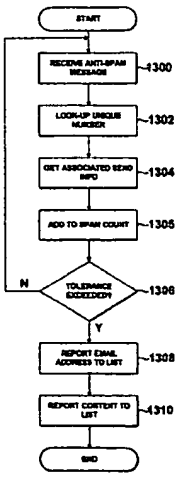
(List continued on next page.)

Primary Examiner—Robert B. Harrell
Assistant Examiner—Hien C Le
(74) *Attorney, Agent, or Firm*—Perkins Coie LLP

(57) **ABSTRACT**

A system, method, and article of manufacture are provided for affording an application program with an electronic message to help preclude unwanted electronic messages from being sent on a network. First, at least one application program is initialized after an electronic message is selected by a user. Such application program is received with the electronic message on a network. After initialization, the application program is executed. The execution of the application program includes displaying text included with the electronic message, depicting indicia, and communicating an identifier of the electronic message on the network upon the selection of the indicia by the user for precluding unwanted electronic messages from being sent on the network.

16 Claims, 9 Drawing Sheets



U.S. PATENT DOCUMENTS

5,832,208	A		11/1998	Chen et al.
5,832,502	A		11/1998	Durham et al.
5,838,790	A		11/1998	McAuliffe et al.
5,848,397	A		12/1998	Marsh
5,856,825	A		1/1999	Yumoto et al.
5,859,636	A		1/1999	Pandit
5,884,246	A		3/1999	Boucher et al.
5,903,269	A		5/1999	Poreh et al.
5,909,545	A		6/1999	Frese, II et al.
5,918,014	A		6/1999	Robinson
5,937,162	A		8/1999	Funk et al.
5,937,392	A		8/1999	Alberts
5,948,061	A		9/1999	Merriman et al.
5,956,486	A		9/1999	Hickman et al.
6,002,393	A		12/1999	Hite et al.
6,014,502	A		1/2000	Moraes
6,014,688	A	*	1/2000	Venkatraman et al. 709/206
6,014,698	A		1/2000	Griffiths
6,055,510	A		4/2000	Henrick et al.
6,067,570	A		5/2000	Kreynin et al.
6,092,104	A		7/2000	Kelly
6,138,149	A		10/2000	Ohmura
6,144,987	A		11/2000	Niemi
6,167,395	A		12/2000	Beck et al.
6,167,434	A	*	12/2000	Pang 709/206
6,199,103	B1		3/2001	Sakaguchi et al.
6,199,106	B1		3/2001	Shaw et al.
6,205,432	B1		3/2001	Gabbard et al.
6,212,554	B1		4/2001	Roskowski
6,219,054	B1		4/2001	Komoda et al.
6,233,317	B1		5/2001	Homan et al.
6,253,231	B1		6/2001	Fujii
6,275,849	B1		8/2001	Ludwig
6,327,612	B1		12/2001	Watanabe
6,332,156	B1		12/2001	Cho et al.
6,351,763	B1		2/2002	Kawanaka
6,400,810	B1		6/2002	Skladman et al.
6,405,244	B1	*	6/2002	Bando et al. 709/206
6,415,332	B1		7/2002	Tuel, Jr.
6,427,164	B1		7/2002	Reilly
6,438,583	B1		8/2002	McDowell et al.
6,449,635	B1		9/2002	Tilden, Jr. et al.

OTHER PUBLICATIONS

The Internet article, "No Junk E–Mail Database" (herein after "No Junk E–Mail") obtained from the World Wide Web address http://www.glr.com/nojunk.html on Sep. 21, 1999.

The Internet article, "What can you do about bad email?" (herein after "Bad Email") obtained from the World Wide Web address http://www.oitc.com/Disney/WhatToDo.html on Sep. 21, 1999.

The Internet article, "The Anti–Spam HOWTO" obtained from the World Wide Web address http://www.zikzak/zikzak.net/~acb/features/anit–spam–howto.html on Sep. 21, 1999.

The copies of pages obtained on Sep. 21, 1999 from the website entitled "Do–Not–Spam.com" located at the World Wide Web address http://www.do–not–spam.com/.

Yourdon, Java, the Web and Software Development, IEEE 1996.

World Wide Web e–mail service provider Hotmail (hereinafter "Hotmail") available through the web site http://www.msn.com provided by the Microsoft Corporation, Exhibit A, pp. 1 through 3 enclosed herewith is a print out of another feature of Hotmail called Mail Handling.

Exhibit B is a print out of a page from Activegrams with the address: http://www.activegrams.com?cgi–bin/viewactivegrams.cgi?dadbday on Sep. 26, 1999.

Real Networks, Inc. (hereinafter "RealNetworks") a comparison with headquarters at 2601 Elliott Avenue, Suite 1000, Seattle, WA 98121, offers a line of products that include Real Player and Real Audio and the like. Versions of these products may be downloaded from the Internet at http://www.real.com.

* cited by examiner

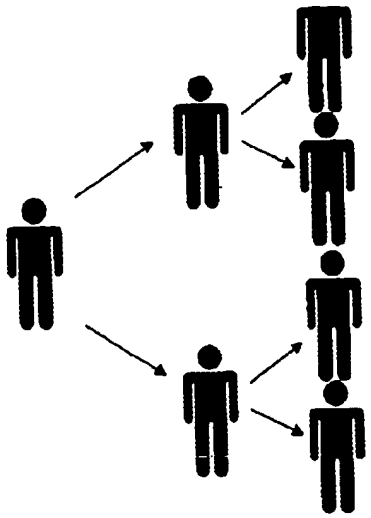


FIG. 1
(PRIOR ART)

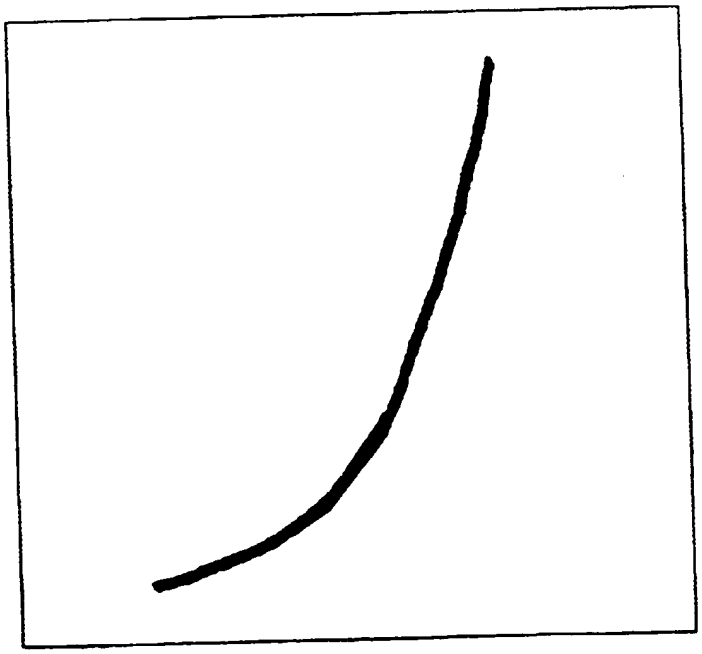


FIG. 2
(PRIOR ART)

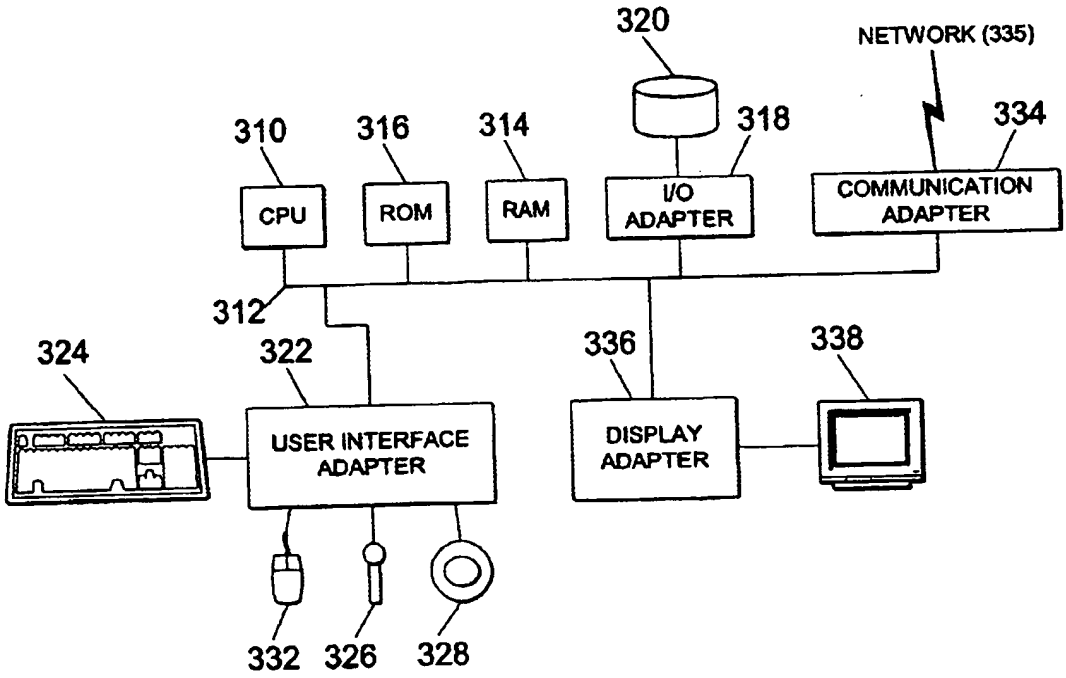

320
NETWORK (335)
310
316
314
318
334
CPU
ROM
RAM
I/O ADAPTER
COMMUNICATION ADAPTER
312
324
322
336
338
USER INTERFACE ADAPTER
DISPLAY ADAPTER
332
326
328

FIG. 3

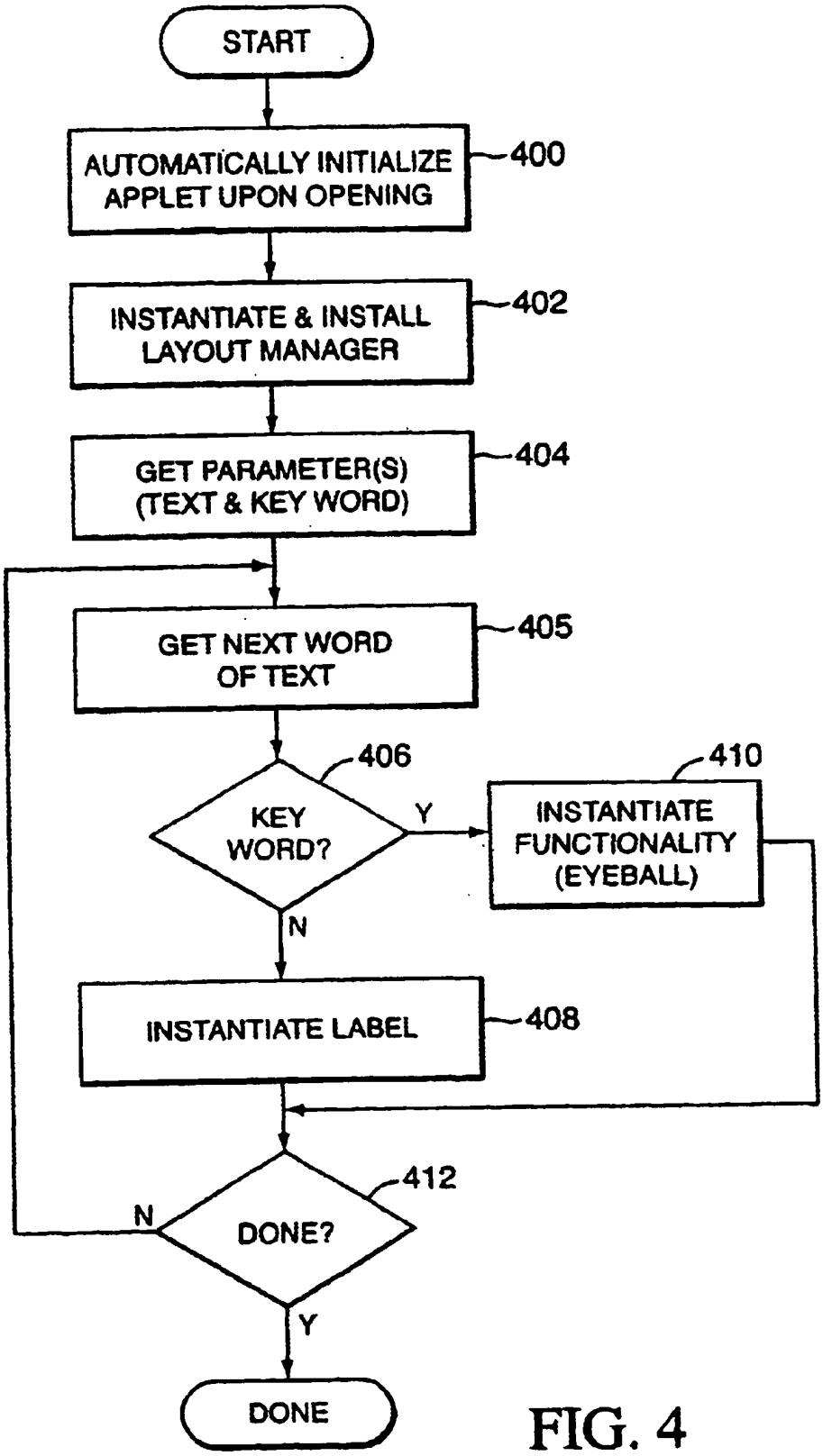

START
AUTOMATICALLY INITIALIZE APPLET UPON OPENING
400
INSTANTIATE & INSTALL LAYOUT MANAGER
402
GET PARAMETER(S) (TEXT & KEY WORD)
404
GET NEXT WORD OF TEXT
405
406
KEY WORD?
Y
410
INSTANTIATE FUNCTIONALITY (EYEBALL)
N
INSTANTIATE LABEL
408
412
N
DONE?
Y
DONE

FIG. 4

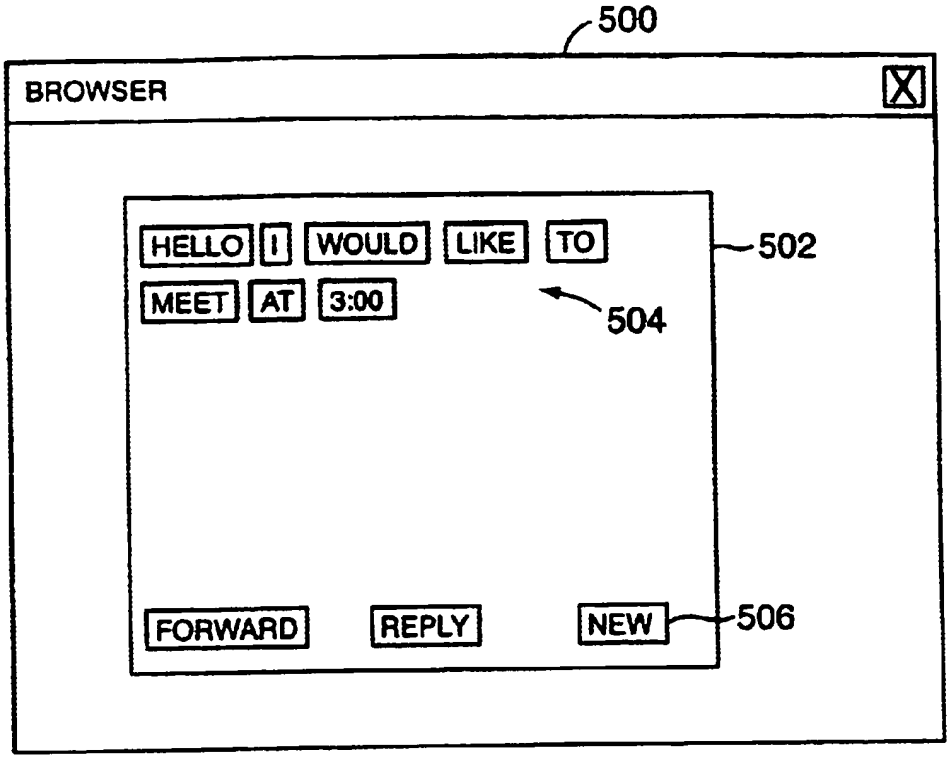

500
BROWSER
HELLO I WOULD LIKE TO
MEET AT 3:00
502
504
FORWARD
REPLY
NEW
506

FIG. 5

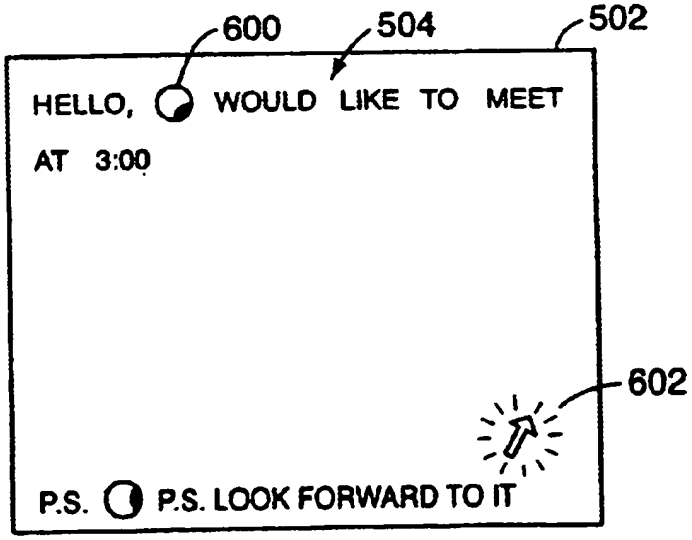

600
504
502
HELLO, WOULD LIKE TO MEET
AT 3:00
602
P.S. P.S. LOOK FORWARD TO IT

FIG. 6

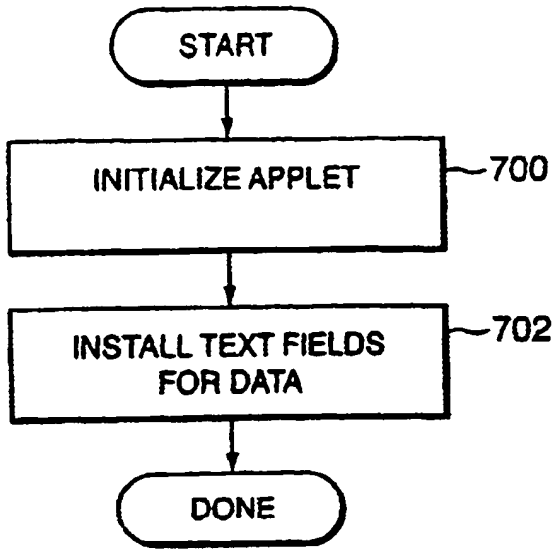

START
INITIALIZE APPLET
700
INSTALL TEXT FIELDS FOR DATA
702
DONE

FIG. 7

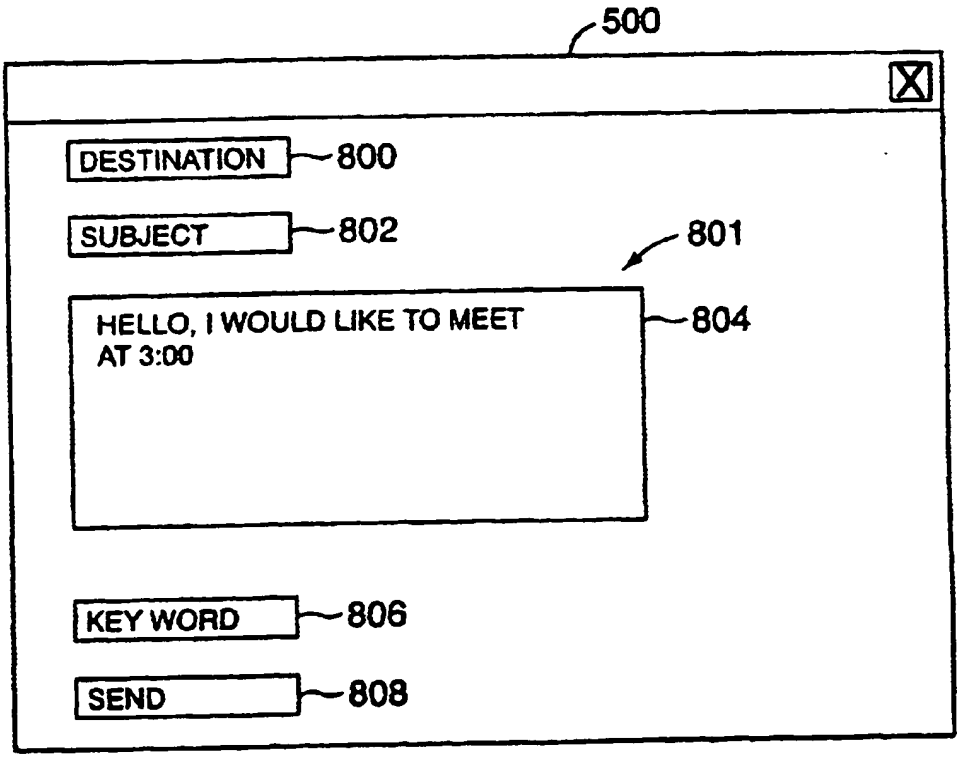

500
DESTINATION
800
SUBJECT
802
801
HELLO, I WOULD LIKE TO MEET AT 3:00
804
KEY WORD
806
SEND
808

FIG. 8

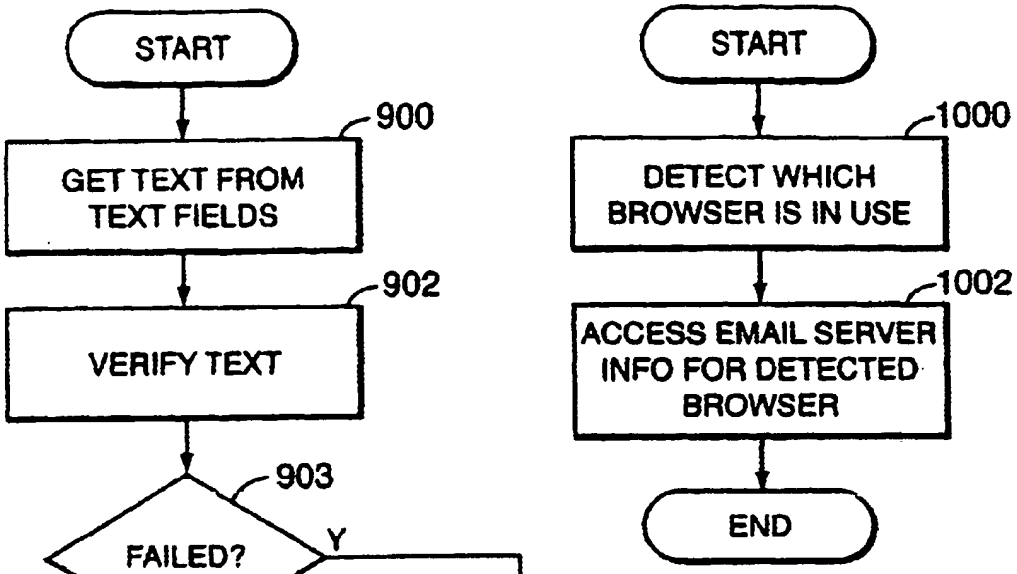

START
1000
DETECT WHICH BROWSER IS IN USE
1002
ACCESS EMAIL SERVER INFO FOR DETECTED BROWSER
END

FIG. 10

START
900
GET TEXT FROM TEXT FIELDS
902
VERIFY TEXT
903
FAILED?
Y
N
905
FETCH EMAIL SERVER INFO FROM DISK
906
FORMAT & SEND MESSAGE
908
MESSAGE SEND OK?
N
Y
910
GOTO WEBSITE
904
COMPLAIN
END

FIG. 9

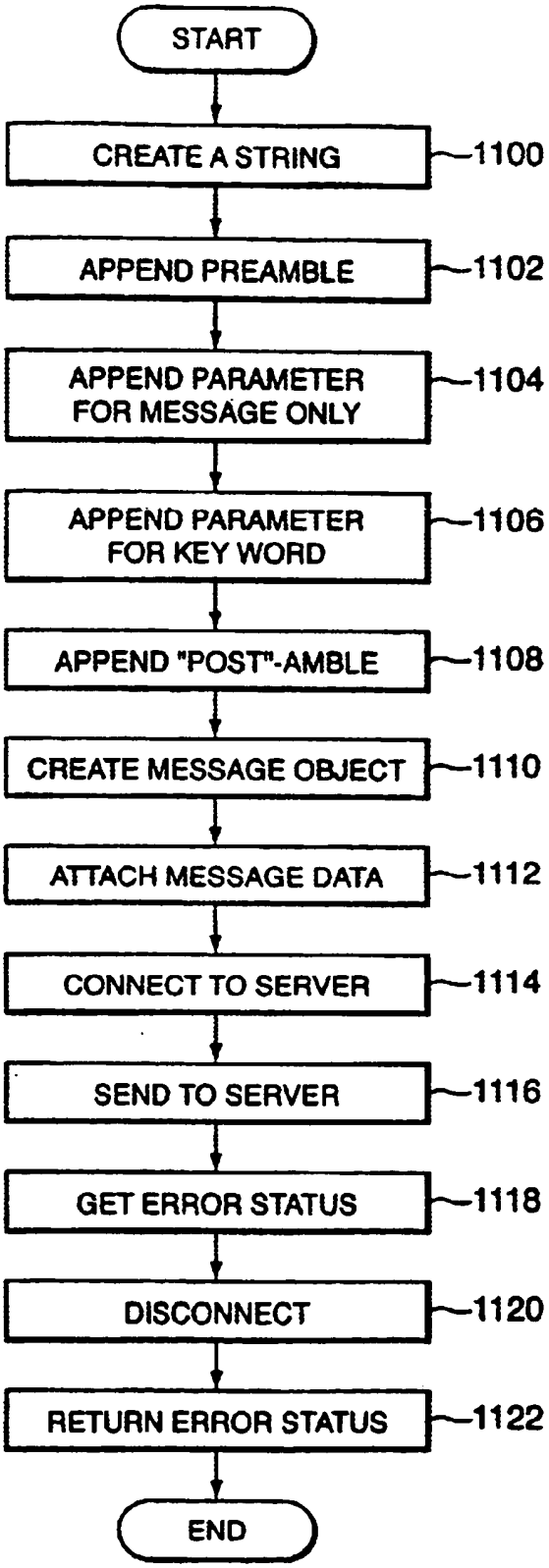

START
CREATE A STRING
1100
APPEND PREAMBLE
1102
APPEND PARAMETER FOR MESSAGE ONLY
1104
APPEND PARAMETER FOR KEY WORD
1106
APPEND "POST"-AMBLE
1108
CREATE MESSAGE OBJECT
1110
ATTACH MESSAGE DATA
1112
CONNECT TO SERVER
1114
SEND TO SERVER
1116
GET ERROR STATUS
1118
DISCONNECT
1120
RETURN ERROR STATUS
1122
END

FIG. 11

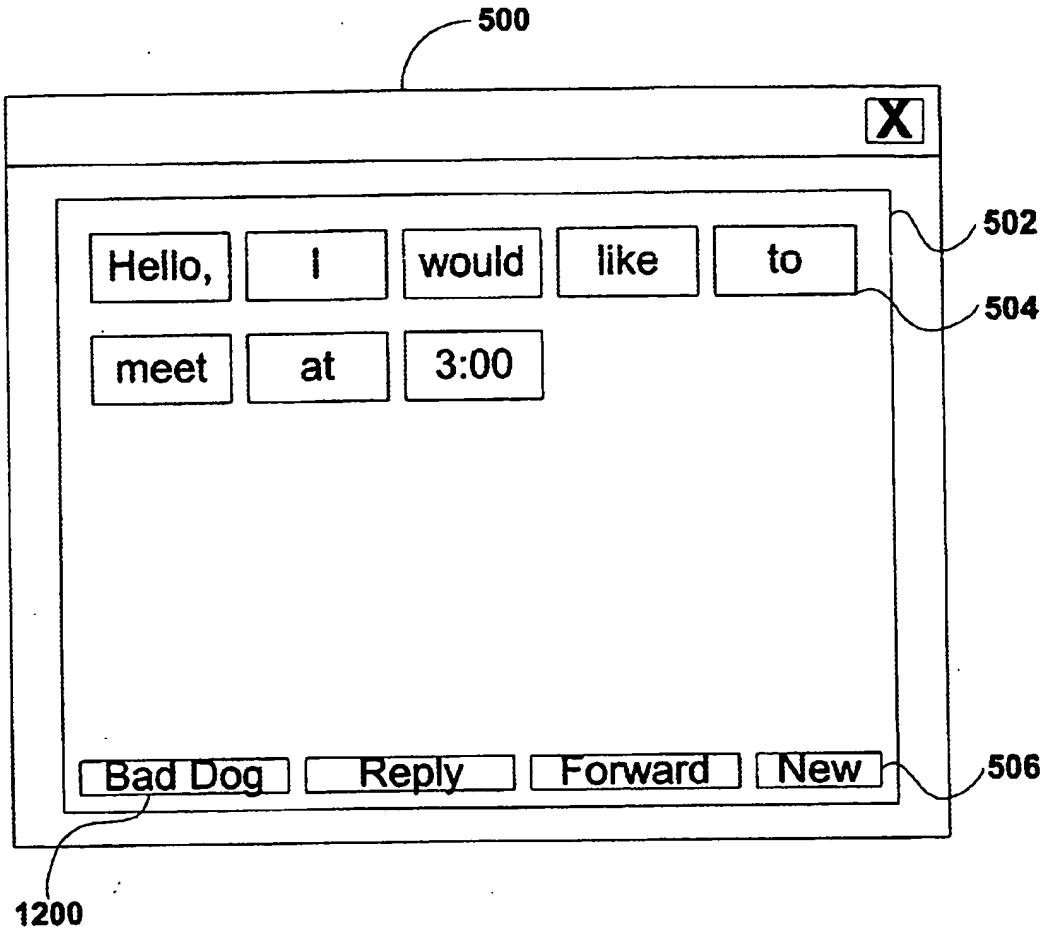

500
X
Hello,
I
would
like
to
meet
at
3:00
502
504
Bad Dog
Reply
Forward
New
506
1200

FIG. 12

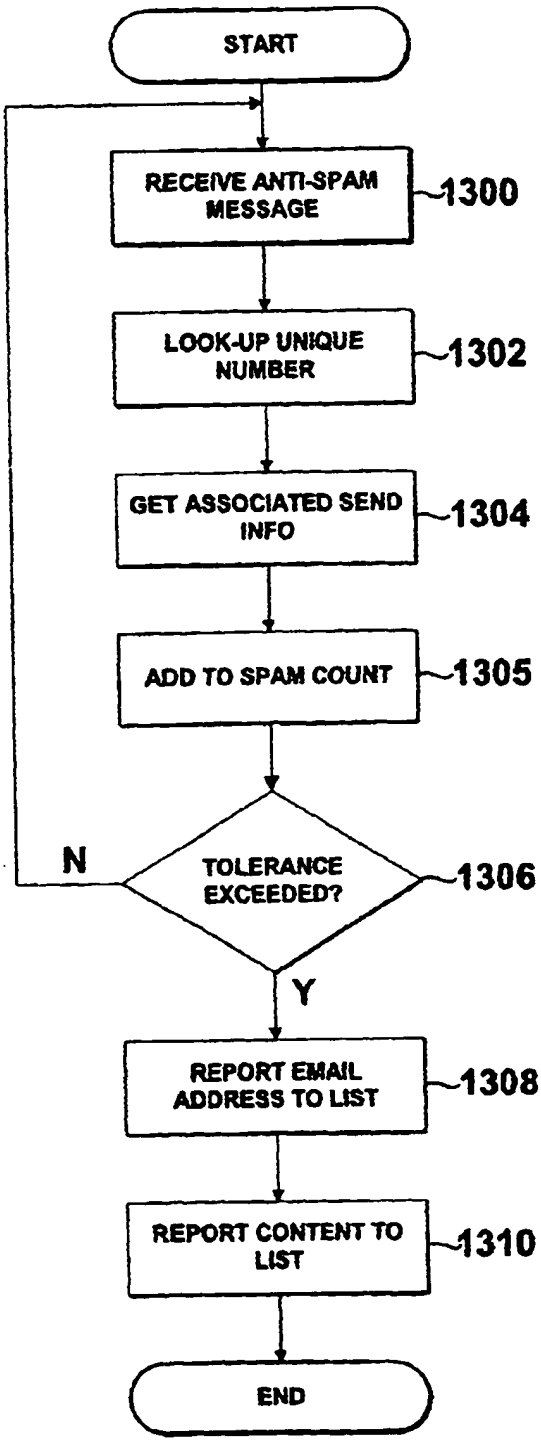

START
RECEIVE ANTI-SPAM MESSAGE
1300
LOOK-UP UNIQUE NUMBER
1302
GET ASSOCIATED SEND INFO
1304
ADD TO SPAM COUNT
1305
TOLERANCE EXCEEDED?
1306
N
Y
REPORT EMAIL ADDRESS TO LIST
1308
REPORT CONTENT TO LIST
1310
END

FIG. 13

SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR PREVENTING THE PROLIFERATION OF UNWANTED ELECTRONIC MESSAGES

RELATED APPLICATIONS

The present application relates to applications entitled "Electronic Message Payload for Interfacing with Text Contained in the Message", "Method and Article of Manufacture for a Sub-Browser Application Program Stored in an Electronic Message", "Method and Article of Manufacture for Delaying Advertisement Execution in a Geometric Electronic Media Distribution Framework", "Textual Hyperlink Capable of Inputting Text as a Parameter while Executing an Associated Link", and "Method and Apparatus for the Production, Delivery, and Receipt of Enhanced E-Mail" which were filed concurrently herewith and are incorporated herein in their entirety.

FIELD OF THE INVENTION

The present invention relates to e-Conmerce and more particularly to preventing unwanted electronic messages, or "spam", from being proliferated on a network.

BACKGROUND OF THE INVENTION

Computer technology is continuously advancing, providing newer computer systems with continuously improved performance. One result of this improved performance is an increased use of computer systems by individuals in a wide variety of business, academic and personal applications. In some instances, these computer systems are linked together by a network or modems so that the systems can communicate with each other via electronic mail.

Electronic mail, or "e-mail", has become a popular way for people to communicate using networks of various types such as the Internet. Using e-mail, a person can send messages and other information as attachments electronically to other e-mail users. Such attachments normally include pictures, sound recordings, formatted documents, etc. that are in digital form, and which are executable independent of the opening and reading of the message included with the e-mail.

The recent explosion in the popularity of the Internet has provided tremendous potential for marketing goods and services. However, for most small to mid-sized companies, advertising their wares and services through a web-site on the Internet has not proven to be very effective. One of the difficulties with advertising on the Internet is directing consumers to visit a particular web-site. The overabundance of web-site locations has created an information overload for many consumers.

E-mail is one possible solution for advertisers. Despite its allure, however, promotional e-mail is still frowned upon, and at present its content is generally limited to unformatted text without graphics which is often not personalized. Accordingly, promotional e-mail is often disregarded, and in almost all cases, is not propagated by the recipients themselves.

At the present, such promotional e-mail, or "spam", has become such an annoyance to many users of e-mail that "lists" have formed. Such lists are often generated by users reporting unwanted e-mail to a central site which, in turn, uses filtering techniques or the like to prevent the proliferation of the unwanted email. While such "lists" are effective once the unwanted e-mail is disclosed, a problem often arises in reporting the unwanted e-mail.

Users are often very busy, and excuse unwanted e-mail rather that reporting the same due to the multiple user actions required for reporting. Namely, a user must often copy the domain name, exit an e-mail browser, initiate a network browser, locate the appropriate "list" site, and manually enter the domain name and any other required information. These tedious steps often serve as a deterrence to take action upon receiving an unwanted electronic message.

SUMMARY OF THE INVENTION

A system, method, and article of manufacture are provided for affording an application program with an electronic message to help preclude unwanted electronic messages from being sent on a network. First, at least one application program is initialized after an electronic message is selected by a user. Such application program is received with the electronic message on a network. After initialization, the application program is executed. The execution of the application program includes displaying text included with the electronic message, depicting indicia, and communicating an identifier of the electronic message on the network upon the selection of the indicia by the user for precluding unwanted electronic messages from being sent on the network.

In one aspect of the present invention, the identifier is generated by a server that sends the electronic message on the network to the user. As an option, the identifier may be stored in the application program to be sent upon the selection of the indicia.

In another aspect of the present invention, an amount of the identifiers that were sent by a plurality of users who received the electronic message may be tracked. Upon a predetermined amount of the identifiers being tracked, unwanted electronic messages may be prevented from being sent on the network.

As an option, the transmission of the unwanted electronic messages may be precluded by preventing the transmission of any subsequent electronic messages from a source of the original unwanted electronic message. Further, content of the electronic message may be received, thus allowing the prevention of transmission of any subsequent electronic messages having content substantially similar to the received content.

These and other advantages of the present invention will become apparent to those skilled in the art upon a reading of the following descriptions of the invention and a study of the several figures of the drawing.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing aspects are better understood from the following detailed description of one embodiment of the invention with reference to the drawings, in which:

FIG. 1 is an illustration of the geometric manner in which an electronic message may be distributed over a network in accordance with the prior art;

FIG. 2 is a graph depicting the geometric nature illustrated in FIG. 1;

FIG. 3 is a schematic diagram of one exemplary hardware implementation of the present invention;

FIG. 4 is a flowchart illustrating the execution of the first application program of one embodiment of the present invention;

FIG. 5 is an illustration of a graphical user interface of the present invention that is displayed upon the execution of the first application program, and which is used to display the text of the first electronic message and any functionality associated therewith;

FIG. 6 illustrates one example of the functionality displayed upon execution of the first application program in accordance with one embodiment of the present invention;

FIG. 7 illustrates the execution of the second application program of the present invention, or in an alternate embodiment, interaction with a site on the network which is initiated upon the selection of one of the "FORWARD", "REPLY", or "NEW" icons displayed in the graphical user interface of FIG. 5;

FIG. 8 is an illustration of a graphical user interface initiated after selection of one of the "FORWARD", "REPLY", or "NEW" icons in accordance with one embodiment of the present invention;

FIG. 9 is a flowchart illustrating the continued operation of the present invention upon the selection of the "SEND" or other similar icon on the graphical user interface of FIG. 8;

FIG. 10 is a flowchart illustrating the operations associated with the fetch e-mail operation of FIG. 9;

FIG. 11 is a flowchart illustrating the operations associated with the format and send message operation of FIG. 9;

FIG. 12 is a graphical user interface similar to that of FIG. 5 with the exception of an additional "unwanted electronic message" icon; and

FIG. 13 is a flowchart illustrating a server-based process initiated upon the selection of the additional "unwanted electronic message" icon of FIG. 12.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIGS. 1 and 2 illustrate the geometric manner in which an electronic message may be distributed over a network in accordance with the prior art. FIGS. 3–13 illustrate a system for providing an application program adapted to be incorporated as a "payload" of an electronic message. Such application program is automatically initialized after the electronic message is selected by a user. After initialization, the application program is executed. The execution of the application program includes various features.

For example, such execution may include displaying text included with the first electronic message, displaying indicia, allowing entry of text, and sending the entered text and the application program over a network in a second electronic message to a second user upon selection of the indicia. In one embodiment, a code segment may be executed which includes as a parameter at least a portion of the text included with the electronic message, thus incorporating the text with any type of functionality, i.e. graphic, etc. Still yet, other features may be included such as an advertisement that is displayed only after the electronic message is forwarded a predetermined number of instances. Also, the text included with the electronic message may constitute a hyperlink which, when selected, links to a site and enters the text as a parameter upon such linking.

As will become apparent, the personal text of the electronic message may induce the user to open the mail while the functionality may serve as an inducement to send the electronic message to another user. This in turn may be used to incur visits to a particular site on the network. In the alternative, it may serve to afford widespread exposure of advertisements or any other feature that supports e-Commerce.

FIG. 3 illustrates an exemplary hardware configuration in accordance with one embodiment having a central processing unit 310, such as a microprocessor, and a number of other units interconnected via a system bus 312. The hardware configuration shown in FIG. 3 includes Random Access Memory (RAM) 314, Read Only Memory (ROM) 916, an I/O adapter 318 for connecting peripheral devices such as disk storage units 320 to the bus 312, a user interface adapter 322 for connecting a keyboard 324, a mouse 326, a speaker 328, a microphone 332, and/or other user interface devices such as a touch screen (not shown) to the bus 312, communication adapter 334 for connecting the hardware configuration to a communication network 335 (e.g., a wide area network) and a display adapter 336 for connecting the bus 312 to a display device 338.

The hardware configuration typically has resident thereon an operating system such as the Microsoft Windows NT or Windows/98/2000 Operating System (OS), the IBM OS/2 operating system, the MAC OS, or UNIX operating system. Those skilled in the art will appreciate that the present invention may also be implemented on platforms and operating systems other than those mentioned.

FIG. 4 is a flowchart illustrating the execution of the first application program associated with the first electronic message that is sent to a first user. The first electronic message may be received over any network such as a wide area network. In one embodiment, such wide area network may include the Internet and the first electronic message may be transmitted using a protocol such as TCP/IP and/or IPX. The first electronic message includes a first application program incorporated therein by any desired technique, along with a message, i.e. graphic, textual, audible, etc., generated by a previous user. In one embodiment, at least a portion of the first application program includes a JAVA APPLET. In the alternative, such first application program may include code segments written in any desired object-oriented computer programming or markup language.

As shown in operation of FIG. 4, the first application program of the first electronic message is automatically initialized upon being selected, or "opened", by a user on an electronic mail browser, i.e. NETSCAPE COMMUNICATOR, MICROSOFT OUTLOOK, etc. Such selection may include "clicking" on an identifier of the first electronic message, or any other technique enabled by the electronic mail browser. Upon such user action, the first electronic message is initialized immediately in an automated manner. To accomplish this, the first application program may depart from an "attachment" in the traditional sense, and be included in the first electronic message itself. Further, the electronic mail browser must be capable of automatically recognizing and executing the computer or markup language employed by the application program, a common capability among electronic mail browsers.

Initialization of the first application program may include determining various variables and other parameters required to execute the application program, or any other "pre-execution" duties. For example, one of such parameters may comprise the body of text included with the first electronic message.

In one embodiment, hypertext markup language may be included with the first electronic message to contain the parameters and call another portion of the first application program such as a JAVA APPLET located at another site on the network. It should be noted, however, that the hypertext markup language itself or any other computer or markup language included with first electronic message may con-

stitute a component or an entirety of the first application program. In other words, any desired portion(including no portion) of the first application program may be positioned at a separate location on the network.

Following is an example of hypertext markup language for containing the parameters and calling another portion of the first application program. In the present embodiment, a portion of the first application program is called using a URL on the network.

```
<HTML>
<HEAD>
<TITLE>Practice Applets</TITLE>
</HEAD>
<BODY>
<APPLET CODEBASE="http://www.esprinkles.com"
CODE="HelloAgainWorld.class" ARCHIVE="eyejar.jar" WIDTH=1000
HEIGHT=1000
ALIGN=left>
<PARAM NAME=info VALUE=" . . . body of text . . . ">
<PARAM NAME=keystring VALUE="I">
</APPLET>
</BODY>
</HTML>
```

In operation **402** of FIG. **4**, execution of the first application program has commenced and a layout manager is instantiated and installed. Layout managers are well known to those of ordinary skill in the art, and function to define the graphical framework during execution. Specifics regarding the graphical framework will be set forth in greater detail in the description of FIG. **5**.

Thereafter, in operation **404**, a particular key string parameter is retrieved in addition to the entire body of text. The key string parameter may include a particular string of text that is included in the body of text. In one embodiment, the word "I" may be retrieved as the key string parameter. In still other embodiments, any other letter, expression, word, phrase, pattern, format, etc. may be used as a key string parameter.

Next, each word and/or phrase of the body of text is retrieved in operation **405**, and compared with the key string parameter to determine whether there is a match in decision **406**. To accomplish this, a parser such as ANTLR may be employed to identify the designated letter, expression, word, phrase, pattern, format, etc. If it is determined that a match does not exist, a convention label is instantiated for simply displaying the current word and/or phrase in operation **408**. On the other hand, if it is determined that a match does indeed exist, a functionality is instantiated which incorporates the key string parameter in operation **410**. It is then determined in decision **412** whether all of the words and/or phrases of the body of text have been compared. If not, the process operations **405–410** are repeated.

FIG. **5** is an illustration of a graphical user interface of the present invention that is displayed upon the execution of the first application program, and which is used to display the text of the first electronic message and any functionality associated therewith. As shown, a frame **500** of the network browser encompasses a text box **502**. Such text box includes the body of text **504**. Further, a plurality of first indicia **506** is displayed in or around the text box. In one embodiment, the first indicia may include a "FORWARD", "REPLY", and/or a "NEW" icon.

FIG. **6** illustrates one example of the functionality displayed upon execution of the first application program. In such embodiment, the key string parameter is "I", and an eyeball **600** is graphically depicted in place of the key string parameter within the textbox **502**. During use, the movement of the eyeball **600** may be adapted to coincide with the movement of a mouse cursor **602**. This may be accomplished using a "mouse listener" which may interface with the first application program. Mouse listeners track a current position of mouse cursors. It should be noted that in various alternate embodiments, any type of user input may be used to change various aspects, i.e. graphic, textual, layout, color, sound, etc. of the first electronic message.

Programs that execute the foregoing eyeball graphic feature are commonly known to those of ordinary skill. Such programs commonly use atan2 in order to compute the angle between the eyeball and the mouse cursor. An example of a code segment that executes the mouse listener feature, and that calls the eyeball graphic feature is as follows:

```
import java.applet.*;
import java.awt.*;
import java.lang.*;
import java.util.*;
import java.awt.event.*;
import java.net.*;
public class HelloAgainWorld extends Applet
{
    Image backBuffer;
    Graphics backG;
    String s = "null";
    public void init()
    {
    //this.setLayout(null);
    this.setLayout(new FlowLayout(FlowLayout.LEFT));
    s= getParameter("info");
    StringTokenizer parser = new StringTokenizer(s);
    try
    {
        while(parser.hasMoreTokens())
        {
            String a = parser.nextToken();
            if (a.equals("I"))
            {
                Eyeball2 eye = new Eyeball2(this);
                eye.setSize(30, 30);
```

-continued

```
                add(eye);
                Clicker click = new Clicker(this);
                eye.addMouseListener(click);
            }
            else
            {
                Label helloLabel = new Label();
                helloLabel.setText(a);
                helloLabel.setForeground(new Color(170, 27, 140));
                add(helloLabel);
            }
        }
    }
    catch (NoSuchElementException e)
    {
    }
}
public void paint(Graphics g)
{
                maintain();
                super.paint(backG);
                    g.drawImage(backBuffer, 0, 0, null);
}
public void update(Graphics g)
{
                    maintain();
                    super.update(backG);
                    g.drawImage(backBuffer, 0, 0, null);
}
void maintain()
{
                    // Maintain the back buffer and the graphics context that is
directed towards the back buffer.
                    {
                        int w = getBounds().width;
                        int h = getBounds().height;
                        // If there is no buffer or it is the wrong width, or it is
the wrong height, then adjust the back buffer.
                        if ( backBuffer == null || backBuffer.getWidth(null) != w ||
backBuffer.getHeight(null) != h )
                        {
                        // Adjust the back buffer.
                        backBuffer = createImage( w, h );
                        // If we have a backBuffer, then make a graphics context
that is directed towards the back buffer.
                        if (backBuffer != null)
                        {
                            // Dispose of any previous graphics context that may
have pointed to a previous back buffer.
                            if ( backG != null )
                            {
                                backG.dispose();
                            }
                            // Now create the graphics context that is directed
to the back buffer.
                            backG = backBuffer.getGraphics();
                        }
                    }
                }
            }
}
class Clicker implements MouseListener
{
    Applet a;
    URL url;
        Clicker(Applet _a)
        {
            a = _a;
        }
        public void mouseClicked(MouseEvent evt)
        {
        }
    public void mousePressed(MouseEvent evt)
    {
    }
```

-continued

```
    public void mouseReleased(MouseEvent evt)
    {
        AppletContext ac = a.getAppletContext();
        try
        {
            url = new URL("http://207.82.252.253/cgi-
bin/linkrd? lang=&hm action=http%3a%2f%2fwww%2eneostar%2ecom");
        }
        catch (MalformedURLException e)
        {
            System.out.println("I was a malformed url");
        }
        ac.showDocument(url);
    }
    public void mouseEntered(MouseEvent evt)
    {
    }
    public void mouseExited(MouseEvent evt)
    {
    }
}
```

It should be noted that any type of functionality may be incorporated during the execution of the first application program. For example, advertisements may be displayed, etc.

FIG. **7** illustrates the execution of the second application program of the present invention which is initiated upon the selection of one of the first indicia **506**, i.e. the "FORWARD", "REPLY", and/or "NEW" icon, displayed in the graphical user interface of FIG. **5**. It should be noted that, in a "server-based" embodiment, selection of one of the first indicia **506** may initiate a link to a site on the network, thus allowing interaction with the site to afford functionality similar to that afforded by the second application program. To accomplish this, each button may be generated using HTML and have a unique URL associated therewith. As an option, a user may simply access the site on the network to send an electronic message without having to first receive a message.

In particular, it will be assumed in the present description that the "NEW" icon has been selected. It should be noted, however, that given the present description it would be well within the ability of one of ordinary skill to implement the "FORWARD" and "REPLY" functions. With respect to the "REPLY" icon, there may be a need for a mechanism of transferring the body of text from the first application program to the second application program. This may be accomplished by a "cookie" or similar metadata-type information.

As shown in FIG. **7**, a second application program is initialized upon the selection of the first indicia **506** in operation **700**. It should be noted that, in one embodiment, the second application program may be a component of the first application program thus rendering a single application program. In one embodiment, the first application program includes an un-signed application program and the second application program includes a signed application program. Still yet, in the server-based embodiment, interaction with the site on the network is effected in lieu of the initialization of the second application program.

Similar to the first application program, initialization of the second application program may include determining various variables, and other parameters required to execute the application program. Next, in operation **702**, text fields are installed for allowing entry of text by the first user.

FIG. **8** is an illustration of a graphical user interface associated with the continued operation of the present invention after the selection of one of the first indicia **506** of FIG. **5**. As shown, a plurality of text fields **801** are displayed within the frame **500** of the network browser. Included are a destination text box **800** for allowing the insertion of an electronic mail address of a desired destination, a subject text box **802** for allowing entry of a subject of a message, a body text box **804** for allowing entry of a body of text or message, and a key word text box **806** which is adapted for allowing entry of the key string parameter. Also included is second indicia **808** which may take the form of a "SEND" icon or the like.

FIG. **9** is a flowchart illustrating the continued operation of the present invention upon the selection of the second indicia **808**, i.e. "SEND", on the graphical user interface of FIG. **8**. As shown, in operation **900**, the text is first retrieved from the text fields **801** of the graphical user interface of FIG. **8**. Next, in operation **902**, the text is verified to ensure that each of the necessary text fields are filled and valid. For example, the text boxes **800** and **804** may be required.

If it is determined by decision **903** that the verification of operation **902** fails, a complaint is issued in operation **904**. Such complaint may take the form of a pop-up window or the like, and may describe the nature of any defects. On the other hand, if the verification of operation **902** succeeds and all of the necessary fields are filled, information associated with an electronic mail server of the first user is retrieved in operation **905**. This may be accomplished by accessing a hard drive of a computer of the first user which is running the network browser and electronic mail browser. The purpose of obtaining this information is to identify a server from which the information in the text fields **801** may be sent in the form of a second message. In the alternative, a single designated server may be automatically identified by the second application program, thus obviating the need to access the hard drive of the computer of the first user.

Upon identifying a server from which the second message is to be sent, the second electronic message may be formatted and sent to a second user in operation **906**. Upon being sent, another verification may be executed in decision **908** in order to ensure that the second electronic message was sent in a satisfactory manner. If successful transmittal of the message is not verified, a complaint may be issued in a manner similar to that discussed hereinabove with respect to operation **904**.

If, on the other hand, successful transmittal of the message is verified in decision **908**, the second application

program may optionally link the first user to a site on the network in operation **910**. Such site may be identified by the second application program. This feature may thus be used to increase a number of visits, or "hits", on a particular site which in itself may warrant substantial consideration.

FIG. **10** is a flowchart illustrating the operations associated with the fetch e-mail operation **905** of FIG. **9**. As mentioned earlier, this may be accomplished by accessing a hard drive of a computer of the first user which is running the network browser and electronic mail browser. Before this may be effected, in operation **1000**, the browser(s) that is currently in use may be detected after which the appropriate information may be accessed in operation **1002**. As an option, permission to retrieve such information may be gained from the first user prior to any action being taken.

FIG. **11** is a flowchart illustrating the operations associated with the format and send message operation **906** of FIG. **9**. The format refers to the hypertext mark-up language of which an example was provided earlier. In order to generate such format, a string is first created in operation **1100**. Thereafter, a preamble is appended to the string in operation **1102**. Thereafter, the body of text and key string parameters are appended in operations **1104** and **1106** after which a postscript is appended in operation **1108**. An example of each of the foregoing appended elements are outlined as follows using the example set forth earlier:

Preamble

```
<HTML>
<HEAD>
<TITLE>Practice Applets</TITLE>
</HEAD>
<BODY>
<APPLET CODEBASE="http://www.esprinkles.com"
(*1st app. program*)
CODE="HelloAgainWorld.class" ARCHIVE="eyejar.jar"WIDTH=1000
HEIGHT=1000
ALIGN=left>
```

Parameter

```
<PARAM NAME=info Value=" . . . body of text . . . ">
```

Parameter

```
< PARAM NAME=keystring VALUE="I">
Note: multiple key strings and adaptive keys may be used to identify the
letter, expression, word, phrase, format, etc.
```

Postscript

```
</APPLET>
</BODY>
</HTML>
```

With continuing reference to FIG. **11**, a message object is then created in operation **1110**; Thereafter, the string and appendages, or message data, is attached to the object in operation **1112** using the JAVA mail API. Using the information collected about the server, a connection is then effected with the desired host mail server (SMTP or the like) in operation **1114** after which the message object and data are sent in operation **1116**. In the case of multiple electronic mail destinations, this operation may be repeated as many times as required. An error status is then retrieved in operation **1118** to enable the decision **908** of FIG. **9**. Next, the server is disconnected in operation **1120** and the error status is returned in operation **1122**. It should be noted that submission of the data may be accomplished in any form submit-type process.

One example of functionality that may be implemented by the first application program was shown in FIG. **6**. It should be noted, however, that any type of functionality may be employed by running a code segment including as a parameter at least a portion of the text included with the electronic message.

In various embodiments, the functionality may include the incorporation of an image, video, a specific graphic feature, or any other type of object for that matter. For example, any type of theme such as rabbits, earthquakes, time, popular icons and trademarks may be employed during the display of the text associated with the electronic message. As an option, such graphics may in some way interact with the text of the electronic message.

For example, where the theme is earthquakes, the text may be shown to shutter or the like. Or, where the theme is rabbits, the rabbits may be shown hopping from word to word. Still yet another example includes dressing or undressing an icon in various attire or providing any other type of feedback based on user input. Further, where the theme is time, a format of a time, i.e. "7:00", may be detected in order to replace the same with an analog clock graphic which corresponds with the detected time.

As an option, the selection of the graphic or icon may initiate a link to a predetermine site on the network. Still yet, the application program may be adapted to allow the object to be substituted with any of the strings of the text while it is being shown. This may be accomplished with a select and "drag" feature.

In another embodiment, the execution of the first application program may include linking a string of the text of the first electronic message with a site on the network. In other words, such string constitutes a hyperlink. In such embodiment, the execution of the first application program may further include automatically inputting the string as a parameter to the site on the network upon selection of the hyperlink for various purposes. In the case where the site is a search engine, the string may be automatically entered as a search term in the search engine upon the selection of the hyperlink, thus prompting immediate reaction by the search engine. One example of an implementation of this concept is as follows:

http://www.search$_{13}$engine.com/?MT=keystring&SM=MC&DV=0&LG=any&DC=10&DE=2&$_{13}$v=2

In still another embodiment, the functionality associated with the electronic messages provides an inducement for sending them to additional users. With this exposure, the present invention may be used to propagate advertisements over the network. First, the electronic message is provided with the application program attached thereto which is capable of displaying an advertisement. As the message is communicated over the network, each instance of such communication is detected.

As such, the number of the instances that the electronic message is communicated over the network may be traced. The advertisement is then displayed after a predetermined number of the instances greater than one has been tracked. By employing this technique, the users will not be thwarted from forwarding the electronic message until after a predetermined geometric propagation has already taken place. It should be noted that the foregoing tracking ability may also be used to base a determination of compensation from the advertiser.

As an option, the predetermined number may be based on a Fibonacci sequence for optimized perpetuance of the electronic message. Further, the predetermined number may be based on a generation of the electronic message. As an option, the advertisement may be displayed by automatically linking to a site on the network.

FIG. **12** is a graphical user interface similar to that of FIG. **5** with the exception of an additional "unwanted electronic message" icon **1200**, or indicia, that is displayed upon execution of the first application program. Upon selection of such indicia, a server-based process is initiated to help preclude unwanted electronic messages, or "spam", from being sent on a network.

To facilitate this, each message that is received by the user is assigned a unique identifier by the server by way of a common gateway interface (CGI) or the like. In one embodiment, such identifier may include a domain name. In yet another embodiment, the identifier may be a number that is randomly generated, but large enough to ensure uniqueness. This number may be stored in the first application as a parameter, or incorporated into the HTML associated with generating the "unwanted electronic message" icon **1200**.

Upon selection of the "unwanted electronic message" icon **1200**, the identifier of the electronic message is communicated on the network to a designated server. For reasons that will soon become apparent, content of the electronic message may optionally also be sent.

FIG. **13** is a flowchart illustrating a server-based process initiated upon the selection of the additional "unwanted electronic message" icon of FIG. **12** and the receipt of the identifier and content by the server. As shown, the identifier and content of the unwanted message are received in operation **1300**. Thereafter, the unique number is looked-up in operation **1302** in order to retrieve associated information on the source of the unwanted electronic message in operation **1304**. In the case where the identifier is a number, such number may be used to ascertain the domain name of the message which may be stored with the identifier at the time of transmission. A counter associated with the domain name or the electronic message itself is then incremented in operation **1305**.

Thereafter, in decision **1306**, a number of identifiers identifying the same unwanted message or messages from the same source(domain name) is tracked for the purpose of determining whether a tolerance has been exceeded. In other words, it is determined whether such occurrences have exceeded a predetermined level. If not, the identifiers are continuously tracked.

If, however, the tolerance has been exceeded, the unwanted electronic message is reported in operation **1308** for preventing proliferation of the electronic message, similar messages, and/or messages from a similar source. In addition to reporting the message, the server itself may even take active measures to filter or eliminate the electronic message, similar messages, and/or messages from a similar source.

As an option, the content of the electronic message may also be reported in operation **1310** to the list, thus allowing the prevention of transmission of any subsequent electronic messages having content substantially similar to the received content. It should be noted that "lists" are commonly known as a means of preventing the proliferation of already identified unwanted electronic messages. Still yet another option may include sending the user a notice that the report has been received.

While this invention has been described in terms of several preferred embodiments, it is contemplated that alternatives, modifications, permutations, and equivalents thereof will become apparent to those skilled in the art upon a reading of the specification and study of the drawings. It is therefore intended that the true spirit and scope of the present include all such alternatives, modifications, permutations, and equivalents.

What is claimed is:

1. A method for providing an application program with an electronic message to preclude unwanted electronic messages from being sent on a network, comprising:

initializing at least one application program after an electronic message is selected by a user, wherein the application program is received with the electronic message on a network; and

executing the application program after the initialization thereof, the execution of the application program including:

displaying text included with the electronic message, depicting indicia,

communicating an identifier of the electronic message on the network upon the selection of the indicia by the user for precluding unwanted electronic messages from being sent on the network;

tracking an amount of the identifiers that were sent by a plurality of users who received the electronic message; and

precluding unwanted electronic messages from being sent on the network upon a predetermined amount of the identifiers being tracked.

2. The method as set forth in claim **1**, wherein the application program is executed on a network browser.

3. The method as set forth in claim **1**, wherein the electronic message is selected on an electronic mail browser.

4. The method as set forth in claim **1**, wherein the identifier is generated by a server that sends the electronic message on the network to the user.

5. The method as set forth in claim **4**, wherein the identifier is stored in the application program.

6. The method as set forth in claim **1**, and further comprising tracking an amount of the identifiers that were sent by a plurality of users who received the electronic message and precluding unwanted electronic messages from being sent on the network upon a predetermined amount of the identifiers being tracked.

7. The method as set forth in claim **1**, wherein the sending of the unwanted electronic messages is precluded by preventing the transmission of any subsequent electronic messages from a source of the electronic message.

8. The method as set forth in claim **1**, and further comprising receiving content of the electronic message, wherein the sending of the unwanted electronic messages is precluded by preventing the transmission of any subsequent electronic messages having content substantially similar to the received content.

9. A computer program embodied on a computer readable medium for providing an application program with an electronic message to preclude unwanted electronic messages from being sent on a network, comprising:

a code segment for initializing at least one application program after an electronic message is selected by a user, wherein the application program is received with the electronic message on a network; and

a code segment for executing the application program after the initialization thereof, the execution of the application program including:

displaying text included with the electronic message, depicting indicia,

communicating an identifier of the electronic message on the network upon the selection of the indicia by the user for precluding unwanted electronic messages from being sent on the network;

a code segment for tracking an amount of the identifiers that were sent by a plurality of users who received the electronic message; and

a code segment for precluding unwanted electronic messages from being sent on the network upon a predetermined amount of the identifiers being tracked.

10. The computer program as set forth in claim **9**, wherein the application program is executed on a network browser.

11. The computer program as set forth in claim **9**, wherein the electronic message is selected on an electronic mail browser.

12. The computer program as set forth in claim **9**, wherein the identifier is generated by a server that sends the electronic message on the network to the user.

13. The computer program as set forth in claim **12**, wherein the identifier is stored in the application program.

14. The computer program as set forth in claim **9**, and further comprising a code segment for tracking an amount of the identifiers that were sent by a plurality of users who received the electronic message.

15. The computer program as set forth in claim **9**, wherein the sending of the unwanted electronic messages is precluded by preventing the transmission of any subsequent electronic messages from a source of the electronic message.

16. The computer program as set forth in claim **9**, and further comprising a code segment for receiving content of the electronic message, wherein the sending of the unwanted electronic messages is precluded by preventing the transmission of any subsequent electronic messages having content substantially similar to the received content.

* * * * *

US006684248B1

(12) **United States Patent**
Janacek et al.

(10) **Patent No.: US 6,684,248 B1**
(45) **Date of Patent: Jan. 27, 2004**

(54) **METHOD OF TRANSFERRING DATA FROM A SENDER TO A RECIPIENT DURING WHICH A UNIQUE ACCOUNT FOR THE RECIPIENT IS AUTOMATICALLY CREATED IF THE ACCOUNT DOES NOT PREVIOUSLY EXIST**

(75) Inventors: **Robert Janacek**, East Hanover, NJ (US); **Mahesh Muchhala**, Kenilworth, NJ (US)

(73) Assignee: **Certifiedmail.com, Inc.**, Springfield, NJ (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/565,287**

(22) Filed: **May 2, 2000**

Related U.S. Application Data

(60) Provisional application No. 60/132,203, filed on May 3, 1999, provisional application No. 60/132,790, filed on May 6, 1999, and provisional application No. 60/198,033, filed on Apr. 18, 2000.

(51) **Int. Cl.**[7] **G06F 15/16**; G06F 15/177

(52) **U.S. Cl.** **709/225**; 709/230; 709/225; 709/217

(58) **Field of Search** 379/93; 707/1, 707/10, 201; 709/203, 206, 207, 224, 229, 247, 217, 220, 219, 222, 225, 230, 232

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,230,048	A	*	7/1993	Moy	707/1
5,566,230	A		10/1996	Cairo	
5,721,825	A	*	2/1998	Lawson et al.	709/203
5,781,901	A	*	7/1998	Kuzma	707/10
5,790,790	A		8/1998	Smith et al.	
5,809,116	A		9/1998	Cairo	
5,815,555	A		9/1998	Cairo	
D399,836	S		10/1998	Wu et al.	
5,956,154	A		9/1999	Cairo	
6,058,168	A	*	5/2000	Braband	379/93.24
6,092,199	A	*	7/2000	Dutcher et al.	713/201
6,128,655	A	*	10/2000	Fields et al.	709/219
6,182,131	B1	*	1/2001	Dean et al.	709/222
6,192,407	B1		2/2001	Smith et al.	
6,275,850	B1	*	8/2001	Beyda et al.	709/206
6,308,222	B1	*	10/2001	Krueger et al.	709/247
6,389,472	B1	*	5/2002	Hughes et al.	709/229
6,442,571	B1	*	8/2002	Haff et al.	707/201
6,463,464	B1	*	10/2002	Lazaridis et al.	709/207
6,487,599	B1	*	11/2002	Smith et al.	709/229
6,490,620	B1	*	12/2002	Ditmer et al.	709/224

FOREIGN PATENT DOCUMENTS

EP	0838774		4/1998	
EP	0869652		10/1998	
EP	0907120		4/1999	
NL	1006667	C6 *	1/1999	G06F/17/60

OTHER PUBLICATIONS

Casey, T.; Roe, M.; Tuck, B.; Wilbur, S.; "Secure automated document delivery", Computer Security Applications Conference, 1989., Fifth Annual, Dec. 4–8, 1989, Page(s): 348–356.*

* cited by examiner

Primary Examiner—Thomas Lee
Assistant Examiner—James K. Trujillo
(74) *Attorney, Agent, or Firm*—Gibbons, Del Deo, Dolan, Griffinger & Vecchione

(57) **ABSTRACT**

A method is provided for secure transmission of a message via a network where a recipient of the message need not be a party to the network or maintain an active address in the network. Instead, new accounts are created dynamically by the system of the invention in response to a message addressed to an unknown user by sender who is a party to the network. In the operation of the method of the invention, messages from a network-party sender addressed to such an unknown user are deposited into a unique account created for the addressed recipient. That addressed recipient is notified via a non-network communication path that a message is stored and available to it at a network address, and is provided instructions for accessing that network address to retrieve its message.

24 Claims, 1 Drawing Sheet

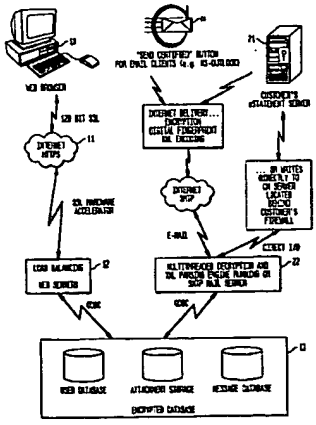
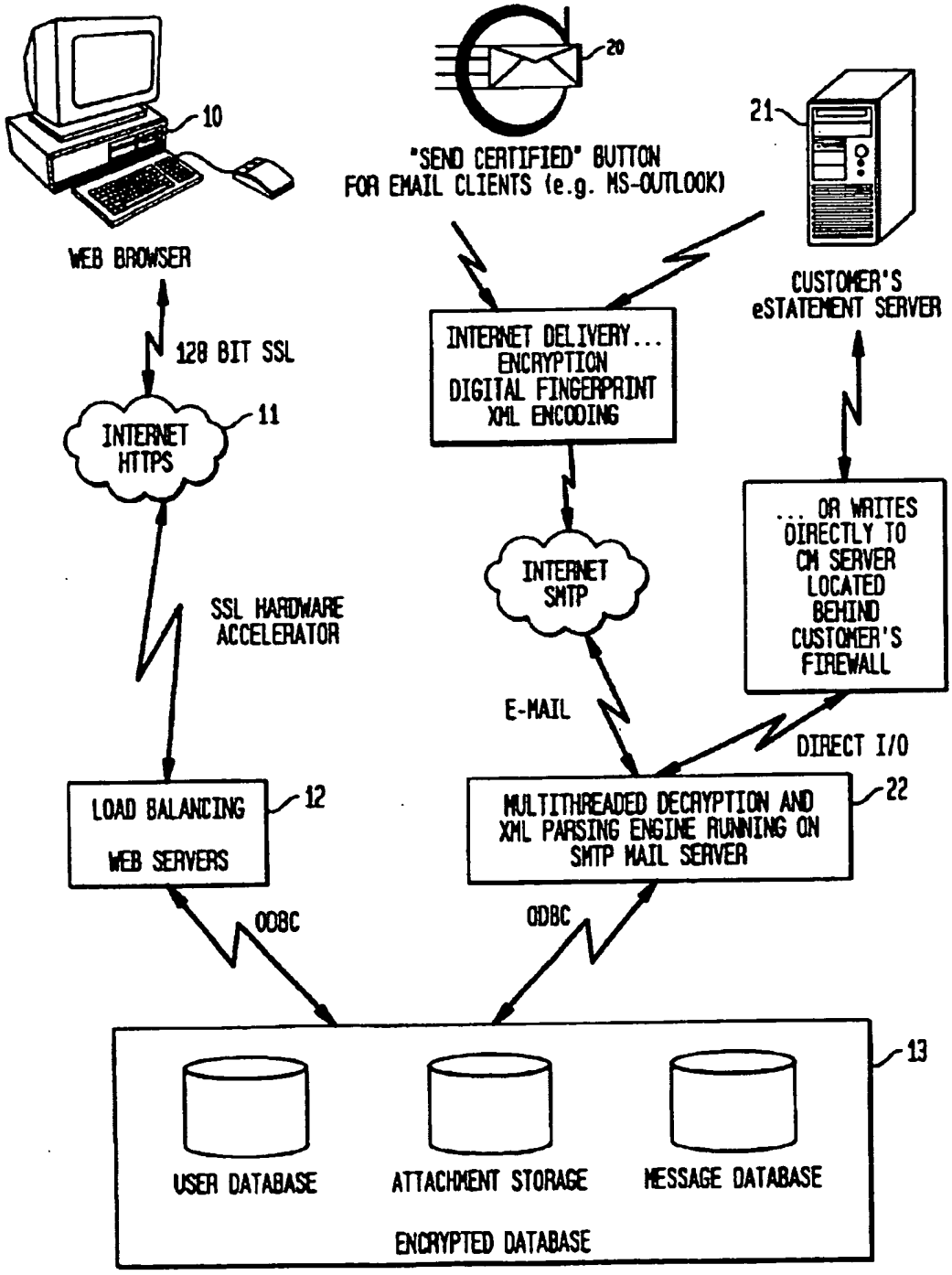


FIG. 1


10
WEB BROWSER
20
"SEND CERTIFIED" BUTTON
FOR EMAIL CLIENTS (e.g. MS-OUTLOOK)
21
CUSTOMER'S
eSTATEMENT SERVER
128 BIT SSL
INTERNET
HTTPS
11
INTERNET DELIVERY...
ENCRYPTION
DIGITAL FINGERPRINT
XML ENCODING
... OR WRITES
DIRECTLY TO
CM SERVER
LOCATED
BEHIND
CUSTOMER'S
FIREWALL
INTERNET
SMTP
SSL HARDWARE
ACCELERATOR
E-MAIL
DIRECT I/O
LOAD BALANCING
WEB SERVERS
12
MULTITHREADED DECRYPTION AND
XML PARSING ENGINE RUNNING ON
SMTP MAIL SERVER
22
ODBC
ODBC
13
USER DATABASE
ATTACHMENT STORAGE
MESSAGE DATABASE
ENCRYPTED DATABASE

METHOD OF TRANSFERRING DATA FROM A SENDER TO A RECIPIENT DURING WHICH A UNIQUE ACCOUNT FOR THE RECIPIENT IS AUTOMATICALLY CREATED IF THE ACCOUNT DOES NOT PREVIOUSLY EXIST

This application claims the benefit of U.S. Provisional Application No. 60/132,203 filed May 3, 1999, U.S. Provisional Application No. 60/132,790 filed May 6, 1999 and U.S. Provisional Application No. 60/198,033 filed Apr. 18, 2000, which are herein incorporated by reference.

FIELD OF THE INVENTION

The present invention relates to computer systems and more particularly to digital messages accessed by computer systems.

BACKGROUND OF THE INVENTION

The Internet is a worldwide system of computer networks—a network of networks in which a user at one computer can obtain information from any other computer (and communicate with users of the other computers). The Internet was conceived by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was first known as the ARPANet. The original aim was to create a network that would allow users of a research computer at one university to be able to communicate with research computers at other universities. To assure that the network could continue to function even if parts of it were destroyed, such as by a military attack or natural disaster, a key design requirement of ARPANet was a facility for bi-directional message routing in a communication link.

The Internet has evolved into a public, cooperative, and self-sustaining facility accessible to hundreds of millions of people worldwide. The most widely used part of the Internet is the World Wide Web (often abbreviated "WWW" or called "the Web"). One important feature of the Web is its use of hypertext documents, a method of instant cross-referencing. On many Web sites, certain words or phrases appear in text of a different color than the rest; often this text is also underlined. When one of these words or phrases is selected, it functions as a hyperlink, transferring the user to the site or page that is linked to this word or phrase. Sometimes there are buttons, images, or portions of images that are "clickable."

Using the Web provides access to millions of pages of information. Web surfing is done with a Web browser; the most popular of which are Netscape Navigator and Microsoft Internet Explorer. The appearance of a particular Web site may vary slightly depending on the particular browser used. Recent versions of browsers have plug-ins, which provide animation, virtual reality, sound, music, and display of text in controlled form.

Because the Internet evolved from the ARPAnet, a research experiment that supported the exchange of data between government contractors and academic researchers, an on-line culture developed that is sometimes alien to the corporate business world. Although the Internet was not designed to make commercialization easy, commercial Internet publishing and e-commerce have rapidly evolved. In part it is the very ease with which anyone can publish a document that is accessible by a large number of people that makes electronic publishing attractive. Setting up an e-commerce site can typically be accomplished with low overhead while providing access to a worldwide market 24 hours a day. The growth and popularity of the Internet is providing new opportunities for commercialization including but not limited to Web sites driven by electronic commerce, ad revenue, branding, database transactions, and intranet/extranet applications.

Domain names direct where e-mail is routed, files are found, and computer resources are located. They are used when accessing information on the Web or connecting to other computers through Telnet. Internet users enter the domain name, which is automatically converted to the Internet Protocol address by the Domain Name System (DNS).

For many Internet users, electronic mail (e-mail) has substantially replaced the Postal Service for written transactions. E-mail is the most widely used application on the Internet. Live "conversations" can be carried on with other computer users, using Internet Relay Chat (IRC). More recently, Internet telephony hardware and software allows real-time voice conversations.

E-mail was one of the first services developed on the Internet. Today, e-mail is an important service on any computer network, not just the Internet. E-mail involves sending a message from one computer account to another computer account. E-mail is used to send textual information as well as files, including graphic files, executable files, word processing and other files. E-mail is becoming a popular way to conduct business over long distances. Using e-mail to contact a business associate can be more effective than using a voice telephone, because the recipient can read it at a convenient time, and the sender can include as much information as needed to explain the situation.

On-line commerce, or "e-commerce", uses the Internet, of which the Web is a part, to transfer large amounts of information about numerous goods and services in exchange for payment or customer data needed to facilitate payment. Potential customers can supply a company with shipping and invoicing information without having to tie up sales staff. The convenience offered to the customer is primarily that of avoiding a trip to one or more traditional "bricks and mortar" establishment in search of a desired product.

The expanding use of e-mail, FTP and other forms of digital message communication is widely displacing traditional paper communications. The Internet is an essential communications tool for individuals, professional users, companies, and government and military agencies. Global interconnectivity and rapid data transfer are among the benefits enjoyed its millions of users. While the Internet provides an undeniably useful environment for data exchange, security is not integrated into its design. In fact, the very concept behind the Internet is a robust open packet communication system.

Therefore, there is a need to provide a system for controlled message distribution.

SUMMARY OF THE INVENTION

A method is disclosed for secure transmission of a message via a network wherein a recipient of the message need not be a party to the network or maintain an active address in the network. Instead, new accounts are created dynamically by the system of the invention in response to a message addressed to an unknown user by sender who is a party to the network. In the operation of the method of the invention, messages from a network-party sender addressed to such an unknown user are deposited into a unique account created for the addressed recipient. That addressed recipient is notified via a non-network communication path that a mes-

sage is stored and available to it, and is provided instructions for accessing a network address to retrieve its message.

DESCRIPTION OF THE FIGURES

FIG. 1 depicts a system embodiment for carrying out the method of the invention.

DETAILED DESCRIPTION OF VARIOUS ILLUSTRATIVE EMBODIMENTS

Vendors, universities and government agencies have attempted to provide a system for controlled message distribution in various ways, with the creation of such security standards as Secure Socket Layer (SSL) and S/MIME. Both of these standards depend on digital certificates, which are at the core of Public/Private Key (PKI) encryption. SSL is often used to securely exchange data between a web browser and an Internet web server. It is a widespread standard since it fills a very clear security hole, and just as importantly, is very easy to implement and use. S/MIME is also a widespread standard, used mainly to secure email messages. But its dependence on unique digital certificates for both the sender and recipient has severely limited its acceptance by email users. With S/MIME, email senders and email recipients must obtain digital certificates and install them in their email client software. Then, the email sender must obtain copies of the Public keys of all of its message recipients, and digitally sign messages with the sender's Private key and each recipient's Public key. While this process produces a secure message exchange between the sender and its recipients, the burden on the sender and recipient has made it too complex for widespread acceptance.

To gain widespread acceptance, secure message delivery over the Internet must be made as technically unchallenging as possible, while still providing uncompromising data protection. Additional value can be added if the sender is notified when its recipients have opened their messages. Further value can be added if the receipt notification works in all cases, regardless of the recipient's email software (e.g. email client, web-based email, personal digital assistant). According to the method of the invention, such a "certified" message delivery system is provided which enables a message recipient to access its account, open its secure electronic mailbox, and quickly access one or more received messages. Upon the recipient opening a message, the system notifies the sender of that event.

In traditional e-mail systems, a user must initiate the account creation process, usually by requesting an account or joining an organization. This is often accomplished by the user visiting a website to fill out a registration form, or by an administrator creating an email address for one or more known users on a system managed by that administrator. Registered users are then assigned a unique email address on the system. In such systems, the user can then send and receive email messages using the assigned e-mail address.

In contrast to this well-established process, with the method of the invention, creation of a messaging account does not require user request, or action by an administrator in respect to a user joining an organization. Instead, new accounts are dynamically created by the system as a result of existing users of the system sending messages to unknown users of the system. Through this unique process, users that may have never had contact with the organization will receive unique password-protected accounts in the system.

Unlike traditional e-mail systems, where messages are delivered into the recipient's messaging system, messages transmitted according to the method of the invention are deposited into a unique account created for the recipient. The messages associated with the account are located on the same system where the message sender established its account. As a result, when the recipient accesses its account to retrieve a message, the system will always know that the message was opened, allowing it to provide the sender with confirmation of that event. In addition, since the message recipient accesses its private account on the system, all other messages sent to the recipient are available to the recipient in an Inbox. This is in contrast to existing message delivery systems. Typical messaging systems can only provide one message to the recipient since the system is based on a unique document ID, and not a unique recipient account. Having unique recipient accounts capable of displaying all received messages significantly increases the usability of the system. It allows the system to achieve the conveniences of conventional email systems, with the security and tracking capability of secure message delivery systems. The dynamic account creation process provided by this invention enables the messaging system to incorporate the benefits and conveniences of email and secure delivery systems. As a result, a messaging system built with this invention provides a unique, superior way to securely deliver and manage documents over the Internet.

The invention utilizes existing e-mail systems for notification of a secured certified message, but actual access is provided to the secured certified message from a database system located at the secured site. The access can be provided through a variety of mechanisms, including a local client, through the use of a web browser, and through the equivalent of plug-in features to existing e-mail systems. By using plug-in features to an existing e-mail system, the creation and access of a secured certified message can be seamless to an e-mail user.

The invention builds upon the fundamental Internet tools such as web browsers, email clients, the manner in which electronic mail is handled on the Internet, the Hypertext Markup Language (HTML), XML and the manner in which Uniform Resource Locators (URLs) work. A significant amount of material describing these features of the Internet is available both through various sites on the Internet and through published resources. Such resources and their applicability to the invention are discussed in the following description of the method and operation of the invention.

Dynamic account and mail store creation capabilities of an electronic document delivery system are among the Internet features utilized by the invention. In this arrangement, recipient accounts are dynamically created as a result of an electronic message being sent by the message sender, whether the sender is a registered user or an application that generates messages (e.g. eBilling, monthly statements). The electronic certified message takes on a familiar email format, and contains one or more individual or Group email addresses in To, CC and BCC fields, a Subject, Body and optionally, one or more file attachments. Recipient email addresses in the To, CC and BCC fields are checked in a case insensitive search against the email addresses of all registered and receive-only users in the system. If an addressed recipient's email address does not already exist, a new account is created for that address. The account is comprised of a unique system-generated user ID (NuID), a username consisting of the recipient's email address, an account password that is randomly generated, and a user type indicating that the addressed recipient is an unregistered receive-only user. The unique user ID (NuID) is used to individually link an account with user data in

various database tables and the file system. A message store is also created for the recipient, and is based on the NuID for the recipient. The first certified message to the recipient (which triggers a receive-only account creation for the recipient), and all subsequent certified messages will then be deposited in the recipient's unique message store.

When a certified message is placed in the recipient's message store, a separate process generates a "mail waiting" email, and sends it via email to the recipient's email address. The "mail waiting" message contains a hypertext web link (hyperlink) pointing to the web server where the recipient's message delivery account can be accessed.

If the certified message is sent to a dynamically created "receive only" user, the "mail waiting" hyperlink will also contain the recipient's username and password as parameters. When the hyperlink is selected, the recipient's web browser will start and access the message system web site. The recipient's username and password are passed as parameters from the hyperlink to the login screen, which authenticates them against the user database and allows entry for the recipient into its account. Once granted entry into the account, the system allows the recipient to access its private message Inbox and retrieve one or more of its certified messages.

If the certified message is sent to the email address of a member that has already registered with the system (e.g. not a dynamically created member), then the "mail waiting" hyperlink will contain the recipient's username but not the password for the recipient. When the user selects the hyperlink, the user's web browser will be started and the message delivery login screen will be displayed. The recipient will then have to provide its login password (as supplied during the user registration) to access its account. Once granted entry into the account, the system allows the recipient to access its private Inbox and retrieve one or more of its certified messages. In addition, since the recipient is already registered with the system, additional features are available, including creating and sending new certified messages.

Method Steps for a Preferred Embodiment

Sequence Flow for Dynamic account creation initiated by a registered member using a web browser:

1. Registered member (member) starts its web browser and accesses the certified message web site (system).
2. Member selects the login web link and login to the system with member's username and password.
3. Member selects the "Create New Message" link.
4. System displays a form with email message fields including recipient fields (To, CC, BCC), Subject, Body and Attachments.
5. Member creates a certified message by filling out the various message fields. In the recipient fields, member provides one or more Internet email addresses in the form username@domain.com. In addition, member can access its address book and select email addresses and predefined Groups of email addresses that it has already created.
6. When ready, the member selects the "Send" button to send the certified message to the recipient(s).
7. The system performs a syntax check of all of the recipient email addresses, ensuring that they are formed as per Internet SMTP email standards. If one or more invalid email addresses are detected, the Send operation is canceled; the system displays an error message and redisplays the message for the member to correct the problem.
8. Upon successfully providing all valid email addresses, and filling out any other required fields such as Subject and Body, when the "Send" button is selected, the system will begin to process the certified message.
9. The system displays a screen that the certified message has been received, and the recipients will be notified that they have a certified message waiting. Unlike conventional email systems, where the recipients receive the sender's message via email, the member's certified message is saved to a database and its attachments, if any, are stored in the file system.
10. Member can then continue using the system and any of its features.
11. Please refer to "Polling Process" for the remaining steps.

Account Creation Polling Process

A process polls the message database at a set interval, searching for certified messages that have not yet been processed. Unprocessed messages have their MsgStatus field set to 1. When one or more of these messages are found, the following steps are taken:

1) The user database is opened, containing email addresses and registration information.
2) The certified message is opened from the message database, and the various recipient email address fields (To, CC, BCC) are accessed.
3) Each email address is checked for correct syntax. Improperly formed email addresses are discarded.
4) One by one, a search is performed, individually looking for each addressed recipient's email address in the email address table of the user database. Since Internet email addresses are case insensitive, the search is case insensitive.
5) If the email address is found in the database, the email address is skipped. The process then repeats step 4 until no more email addresses are found in the recipient fields of the message.
6) If a match is not found, a new "receive only" account must be created for the recipient.

Following are the Steps the System Performs to Dynamically Create this New Account

a) The account initialization process is started. It is comprised of the following steps:
   i) The email address is assigned to a string variable named EMAILADDRESS. Any upper and lowercase characters are left as is, since subsequent searches on the email address will disregard the case of the characters.
   ii) A random password is generated for the account, consisting of 8 alphanumeric characters. It is then assigned to a string variable named PASSWORD. Alphanumeric characters consist of the letters A to Z, and 0 to 9. To ensure that new passwords do not fall into a pattern, the RANDOMIZE function is used, initialized with a numeric value representing the current date and time. Since the date and time are never the same, generating a random value using this method ensures that the computer can generate true random numbers. The computer's RND (random) function is then used to generate the actual random values for the password.
   iii) The system date is queried, and the current date and time are inserted into a string variable named DATECREATED.
   iv) A USERTYPE integer variable is assigned a value of 1. This value is a code used by the messaging system representing the send and receive privilege of the user. A value of 1 signifies that the account is allowed to receive messages, and that an account

login is provided for user access to the messages. Furthermore, a value of 1 signifies that the user can access, display and delete its received messages, but cannot create and send new messages. If the "receive-only" user successfully registers with the messaging system at a later time, their USERTYPE account code will be set to 2 or higher, indicating that the user has both send and receive capability.

v) An SQL database statement is created with this information, and an SQL function is called that writes this information to the user database.

b) Upon adding the entry, the system returns an account ID (NuID) for the newly created user. This NuID is automatically created by the database, and is unique to this user. The user's NuID uniquely correlates the user's account with messages sent to the user and messages the user may generate, store and send.

7) The MsgStatus field of the Message is then set to 2, indicating that all recipient email addresses have been processed, and any new "receive only" accounts have been created.

Message Delivery Polling Process

An independent process polls the message database at a set interval, searching for certified messages that have had their email addresses processed into user accounts but have not yet had "mail waiting" email notices sent to the addressed recipients. These messages will have their MsgStatus field set to 2. When one or more of these messages are found, the following steps are taken:

1) Certified messages with a MsgStatus field set to 2 are accessed one at a time in the database

2) NoticeTimer Subroutine( )

Call NotificationMessage

Select Message where MsgStatus=1

If Not EOF then

Call ProcessMessage

ReadMessage (read message fields)

Increment Sender Messages Sent Counter

Syntax check Message Email Addresses

Store valid Email Addresses into an Array

For each Email Address in the Array

Call DoMessageStatus

Check if account exists for Email Address

If it does not exist:

Set User Type flag to "Receive Only User"

Generate random 8 character password for account

Add a row into the user database

New user's unique account # is generated and returned by the database

If it does exist:

Retrieve user account # from user database

Retrieve UserType field from database

Retrieve UserName field from database

Insert message sender account #, message #, recipient account # and recipient email address into the MsgStatus database

Call DoMessageNotify

End If

Call DoMessageWaitingNotice

Rather than allowing access to a single message as an isolated event, the present invention allows a message recipient to view all messages sent to the recipient. After the message sender's message is processed by the system, and any receive-only accounts are created for new email addresses contained in the sender's message, each message recipient is notified via email that it has a message waiting. The email notice contains an embedded web link back to the message sender's messaging system. In addition, the link contains the recipient login information, including its account name and password. The account name uniquely identifies the recipient to the system, and is made up of its email address. By selecting this embedded web link in its email message, the recipient's web browser is launched. The recipient's account name and password are passed to the login screen of the message system's web server. The web server then authenticates the login against the user database. Upon successful login, the recipient is then provided access to its account. At this point, the recipient is guided to its private Inbox. This Inbox contains the sender's message for retrieval by the recipient. In addition, because the recipient has a unique account ID, any other messages sent to the recipient will also be displayed in the Inbox.

Implementation of Embodiments of the Invention

FIG. **1** illustrates a system implementation for two embodiments of the secure messaging system of the invention. It is noted that users operating under those embodiments can access the encrypted database simultaneously. In one of the embodiments, which is indicated as providing access to the system via a web browser **10**, a secure web connection (SSL) is made via an HTTPS Internet connection **11** to a messaging web server **12**. The browser **10** is used to communicate with the messaging web server **12**, and can create and retrieve secure messages. The web server **12** writes and reads data from/to encrypted database **13** using an ODBC database connection. In the second embodiment, an XML parsing engine **22** is used to receive data, either from a "Send Certified" button **20** installed in an email client (via an SMTP Internet connection), or from an application **21** that generates XML files to be processed by the secure messaging system. The XML parsing engine **22** then writes data to the encrypted database **13** via an ODBC database connection.

One embodiment of the present invention is a method and system for the dynamic creation of user accounts and corresponding message store for the delivery of electronic messages. A message store is also created for these new user accounts, where one or more electronic messages can be retrieved. User account creation is accomplished by the action of an existing registered member or registered process. When an electronic message is sent to an unregistered user, the user is automatically registered with the system, a unique, password-protected account is created and assigned to the user, and a private mail store is created for the user. The electronic message is then deposited into the user's mail store for later retrieval by the user. This is in contrast to traditional electronic mail systems, which require a user to initiate a request for the creation of an account and mail store. Then, at a later time, the user can access its account and mail store to retrieve any deposited messages.

In another embodiment, the invention can provide a certified COD system. The secure, trackable nature of the CertifiedMail architecture can be applied in business-to-business, business-to-government, business-to-consumer, and consumer-to-consumer payment solutions. In such an embodiment, a seller registers with the CertifiedMail system. After registration, the seller can create an invoice on the system, provide payment details, and then furnish the email address of the buyer. The CertifiedMail system creates an inbox for the recipient if one does not already exist, deposits the sender's invoice into the inbox, and sends an email notice that the invoice is waiting to be accessed. When the

recipient opens its message, the sender's invoice is displayed. The recipient is presented with the option of paying for the invoice through various payment types including credit card and check. Upon entering of the recipient's payment information, the CertifiedMail system performs the funds transaction. It then notifies the message sender that the payment has been received. The seller can then ship the purchased goods, or the CertifiedMail system can be instructed to enable the buyer to download the goods from the CertifiedMail message. At a regular interval, CertifiedMail will transfer the collected funds to the seller, minus any transaction fee.

In yet another embodiment, the invention can be used to provide long-term document escrow. The CertifiedMail system provides selectable message expiration periods, including the option of long-term document storage and retrieval. This enables a message to be retrieved after a significant time period for future reference. In addition, when a message is submitted to the system, a mathematical calculation of the message contents, such as Message Digest 5 (MD5), is performed. This calculation is associated with the message, and stored in the database. At a later time, when the message is accessed, the same calculation is performed on the message contents. If the calculation is equal to the value that was originally computed, then the message content is also proven to be identical. In practical use, this computation proves that the message retrieved is equal to the message that was submitted. This creates a system with long-term document retrieval and proof of authenticity.

In yet a further embodiment, the invention can provide secure digital product distribution. Traditional Internet shopping carts store a user's purchases for the duration of that Internet session. However, since digital downloads such as software and newsletters do not include a physical delivery, it is often useful for a purchaser to access its purchase again at a later time. This is especially true when a software purchaser's hard drive crashes, or a new operating system version is installed. The CertifiedMail system provides a repository for storing digital downloads, allowing the purchaser to easily retrieve all past purchases from the CertifiedMail inbox. Any previous or future "email waiting" notice sent by the system to the purchaser allows a secure opening of the purchaser's inbox, providing the purchaser with convenient access to all prior purchases, with the ability to verify each download's authenticity via an automatic digital checksum, and download the contents again.

Additionally, wireless devices are an increasingly popular way to browse the internet. Because of the unique nature of wireless communication, including limited bandwidth and screen display size, the web standard HTML language is not used by most wireless phones. New protocols, such as Wireless Application Protocol (WAP) and Hand-held Device Markup Language (HDML) address these unique characteristics, and are used to send and retrieve web-based information. A wireless interface to the CertifiedMail system enables secure delivery, trackable delivery of messages via the Secure Socket Layer (SSL) web security protocol, which is then converted by the wireless gateway to a secure wireless protocol such as Wireless Transport Layer Security (WTLS), extending the security to the individual wireless device. The CertifiedMail tracking system can detect either the phone number of the wireless device receiving the message, or the IP address assigned to the device.

Since faxes are a form of digital content, they can provide additional security in delivery and tracking beyond what is available via standard fax solutions. Faxes are converted to images, which are then added as attachments to a CertifiedMail message. The recipient is notified via email that a fax is waiting, and the CertifiedMail secure mechanism is used for the recipient to pickup the fax. The fax sender then knows that the fax has been retrieved via the CertifiedMail message tracking.

CertifiedMail provides a system approach to secure messaging, enabling end-to-end security and tracking of confidential messages. This approach makes it ideal for delivering stock trade confirmations, monthly statements and other sensitive financial documents. Because of its end-to-end secure approach, it can replace the requirement to physically print and mail via postal delivery such sensitive documents, significantly reducing the expense of transaction confirmation.

When a member of the CertifiedMail system sends a secure message, a new account may be created by the system for the recipient to pickup the message, or a previously created recipient's account will be used to deposit the new message. As is often the case with messages, the recipient may want to reply to the sender. The CertifiedMail system allows the recipient, who is not a member of its secure delivery system, to reply to the sender using the full security of the CertifiedMail system, thus providing secured two-way communications between the member and the message recipient. This extends the CertifiedMail message delivery security to recipients that were not registered on the system. It is ideal for many two-way communication scenarios including doctor to patient communication, lawyer to client communication, and any member to non-member communication.

Appendix A provides a description of one embodiment the database structures utilized to implement the secured certified message system. Appendix B contains an XML document representative of one embodiment of an external interface utilized with the database structures to provide an interface to other systems such as e-mail systems, intelligent agents and user clients.

In view of the foregoing description, numerous modifications and alternative embodiments of the invention will be apparent to those skilled in the art. Accordingly, this description is to be construed as illustrative only and is for the purpose of teaching those skilled in the art the best mode of carrying out the invention. Details of the structure may be varied substantially without departing from the spirit of the invention, and the exclusive use of all modifications, which come within the scope of the appended claim, is reserved.

APPENDIX A

CMUsr Database

Stores all user related information, including user registration and email address, user's address book and various statistics about the user.

userEmail table:

Stores unique email addresses for registered and non-registered users, and assigns unique account #s (NuID field) to each address. NuID is the common link between a user and messages they send and receive, along with various other related information such as their address book, preferences and payment information.

APPENDIX A-continued

userEmail

	Column Name	Datatype	Length	Precision	Scale	Allow N
🔑	NuID	int	4	10	0	
	emailAddr	varchar	64	0	0	
	userID	varchar	20	0	0	
	password	varchar	10	0	0	
	user Type	tinyint	1	2	0	
	dateCreated	smalldatetir	4	0	0	
	dateLastVisit	smalldatetir	4	0	0	
	numVisits	int	4	10	0	
	msgReceived	int	4	10	0	

Key fields:

NuID — Unique account # generated each time an email address record is added to the table

emailAddr — The email address of all message senders (registered users) and recipients. This field can only contain unique values.

userID — The username required to login to a particular message store. For receive-only accounts, this field is blank and their email address is used as the user name.

password — Along with a username, this password value must be provided to login to a user's account.

userType — Flag which indicates the status of the users, from receive only, free personal or paying

dateCreated — The current date and time that an email address record is added to the database

dateLastVisit — The date and time of the user's last login to the system

numVisits — The number of times the user has logged into the system

msgReceived — The number of messages received by the user

users table:

Stores registered users information including name and address, and several system metrics fields.

users

	Column Name	Condensed Type	Allow Null	Identity
🔑	NuID	int		
	salutation	varchar(10)	✓	
	fName	varchar(25)	✓	
	mi	char(1)	✓	
	lName	varchar(25)	✓	
	companyName	varchar(45)	✓	
	title	varchar(30)	✓	
	phone	varchar(15)	✓	
	extension	varchar(6)	✓	
	address1	varchar(50)	✓	
	address2	varchar(30)	✓	
	city	varchar(25)	✓	
	state	char(2)	✓	
	province	varchar(12)	✓	
	zip	varchar(11)	✓	
	country	char(2)	✓	
	msgSent	int	✓	
	verified	tinyint	✓	
	accountsize	int	✓	
	prSent	int	✓	
	cobrand	varchar(8)	✓	
	cmplan	varchar(10)	✓	
	cmplus	int	✓	
	cmminus	int	✓	
	msgexp	int	✓	
	ca	int	✓	
	CoID	int	✓	
	Admin	bit	✓	
	AdminVerify	bit		
	Registered	bit		

Key fields:

NuID — Taken from the userEmail database, the NuID links the user's information

APPENDIX A-continued

msgSent — Tracks total number of messages sent

verified — When a user registers with CertifiedMail, a message with an embedded web link is sent to their registered email address. By selecting the web link, the user shows that the email address they have provided is their actuai email address. When selected, their account is now activated and they can send CertifiedMail messages.

accountsize — indicates the space in Mb allocated for storage of the user's sent mail messages and attachments

cobrand — If a user was referred to the CertifiedMail site from a cobranding partner's site, the cobranding id of the partner's site will be written to this field.

cmplan — indicates which messaging plan the user has joined, enabling the system to activate or disable certain features, and control disk space usage limitations

cmplus — provides a mechanism to add additional features to the user's existing plan

cmminus — provides a mechanism to subtract features from a user's existing plan

msgexp — provides a default expiration period for messages created by the user

CoID — indicates the company id, if any, with which the user is associated

Admin — indicates whether the user is an administrator for other CertifiedMail user's in their company

Address Book tables:

Stores address book information for each registered user

Key fields:

NuID — Unique user account #

ELID — Unique email list #

ABEmailList

	Column Name	Condensed Type	Allow Nulls	Identity
🔑	ELID	int		✓
	NuID	int		
	fname	varchar(25)	✓	
	lname	varchar(25)	✓	
	company	varchar(35)	✓	
	emailAddr	varchar(64)	✓	

ABGroupList

	Column Name	Condensed Type	Allow Nulls	Identity
	GRID	int		✓
	NuID	int		
	name	varchar(40)		

ABGroupMember

	Column Name	Condensed Type	Allow Nulls	Identity
	GmID	int		✓
	GrID	int		
	ELID	int		
	NuID	int		

CMMSg Database

Stores message related information, including message recipients, subject, body and metrics. Also stores pointers to message attachment files.

Message table:

Stores all messages entered into the system

APPENDIX A-continued

Message

Column Name	Datatype	Length	Precision	Scale	Allow Nulls
NmId	int	4	10	0	
NuID	int	4	10	0	
msgStatus	tinyint	1	3	0	
createTime	datetime	8	0	0	
createIP	varchar	20	0	0	
dateExpire	smalldatetime	4	0	0	
subject	varchar	80	0	0	
fromEmail	varchar	64	0	0	
toEmail	varchar	1024	0	0	
ccEmail	varchar	1024	0	0	✓
bccEmail	varchar	1024	0	0	✓
body	text	16	0	0	✓
question	varchar	64	0	0	✓
answer	varchar	16	0	0	✓
msgsize	int	4	10	0	
numto	int	4	10	0	✓
numread	int	4	10	0	✓
anonymous	tinyint	1	3	0	
emailreceipt	tinyint	1	3	0	
priority	tinyint	1	3	0	
https	tinyint	1	3	0	
encrypt	tinyint	1	3	0	
checksum	varchar	32	0	0	✓
retract	tinyint	1	3	0	✓

Key fields:

NmId	Uniquely generated ID for this message
NuID	Account ID of user creating the message
msgStatus	Stores the status of the message (e.g, ready for processing, delete, retract)
createTime	Creation time of the message
createIP	IP address of the message creation
dateExpire	date that the message expires
subject	the Subject of the message
fromEmail	the email address registered by the user at the time the message is sent
toEmail	recipient To: list containing one or more email addresses, or name of an email address list group
ccEmail	recipient CC: list similar to the toEmail field
bccEmail	recipient BCC: list similar to the toEmail field. When a recipient picks up a message, following conventional email standards, the information in this field is not displayed
body	contains the body of the message
question	contains the text for an optional challenge/response hint. This text is displayed to the recipient when a message is password protected.
answer	contains the response to the challenge question required to open the message
msgsize	contains the size in bytes of the message contents including its attachments
numto	displays the number of emailaddress in the emailTo, emailCC and emailBCC fields
numread	displays the number of recipients that have read the message
anonymous	determines whether the sender's identity is included in the "message waiting" email notice sent to each recipient
emailreceipt	determines whether the system sends an "message read" email to the message sender when each recipient accesses the message
priority	sets the email priority of the "message waiting" email notice sent to each recipient
https	determines whether the recipient is forced to retrieve a message with an https (SSL encrypted) connection to the web server
encrypt	determines whether the message is encrypted when stored on the server
checksum	stores the MD5 checksum of the entire message when received by the system
retract	determines whether an unopened message has been retracted by the message sender, preventing the recipient from opening the message

APPENDIX A-continued

MessageStatus table:

Stores tracking information for each recipient of each message

MessageStatus

Column Name	Datatype	Length	Precision	Scale	Allow Nulls
NmsID	int	4	10	0	
NmID	int	4	10	0	
NuID	int	4	10	0	
NtoId	int	4	10	0	
toEmail	varchar	64	0	0	
msgSent	tinyint	1	3	0	
dalNoOpen	tinyint	1	3	0	✓
openIP	varchar	16	0	0	✓
openTime	datetime	8	0	0	✓
errorSend	varchar	50	0	0	✓
msretract	tinyint	1	3	0	✓

Key fields:

NmsId	Unique id of each message status record in the table
NmId	Message id copied from the Message table
NuId	User account id copied from the useremail table
NtoId	Recipient account id copied from the useremail table
ToEmail	email address of one recipient tracked by this record
MsgStatus	determines the status of the message sent to this user (e.g. not opened, opened, deleted)
delNoOpen	determines whether the message was deleted without the recipient opening it
openIP	holds the IP address of the recipient's computer where the message was opened
openTime	holds the date and time that the recipient opened the message
errorSend	reserved for future use
msretract	determines whether the message sender has retracted the message before the recipient has opened it

FileAttach table:

Tracks links between messages and their file attachments stored in the CertifiedMail database file system

FileAttach

Column Name	Datatype	Length	Precision	Scale	Allow Nulls
NmID	int	4	10	0	
NuID	int	4	10	0	
uname	varchar	25	0	0	
aname	varchar	96	0	0	
fsize	int	4	10	0	

Key fields:

NmID	copied from the Message table, this field links the file attachment record with a particular message
NuID	records which user created this file attachment
uname	unique name of the file attachment as stored in the CertifiedMail database file system
aname	the actual name of the file as submitted to the system
fsize	the actual size of the file in bytes

APPENDIX B

```
<?xml version="1.0" standalone="yes"?>
<!--Note: All data between tags must be Base64-encoded-->
<!DOCTYPE Contents [
    <!ELEMENT Contents (Internal, Message)+>
    <!ELEMENT Internal (Regcode+, CoBrand?, EmailReceipt?, SSL?)+>
    <!ELEMENT Message (To+, CC?, BCC?, From+, Subject+,
                Body?, Attachments?)+>
    <!ELEMENT Attachments (Attachment*)?>
    <!ELEMENT Attachment (AttachName+, AttachFile+)?>
```

APPENDIX B-continued

```
    <!ELEMENT RegCode (#PCDATA)>
    <!ELEMENT CoBrand (#PCDATA)>
    <!ELEMENT EmailReceipt (#PCDATA)>
    <!ELEMENT SSL (#PCDATA)>
    <!ELEMENT To (#PCDATA)>
    <!ELEMENT CC (#PCDATA)>
    <!ELEMENT BCC (#PCDATA)>
    <!ELEMENT From (#PCDATA)>
    <!ELEMENT Subject (#PCDATA)>
    <!ELEMENT Body (#PCDATA)>
    <!ELEMENT AttachName (#PCDATA)>
    <!ELEMENT AttachFile (#PCDATA)>
]>
<Contents>
    <Internal>
        <RegCode/>
        <CoBrand/>
        <EmailReceipt/>
        <SSL/>
    </Internal>
    <Message>
        <To/>
        <BCC/>
        <From/>
        <Subject/>
        <Body/>
        <Attachments>
            <Attachment>
                <AttachName/>
                <AttachFile/>
            </Attachment>
            <Attachment>
                <AttachName/>
                <Attach File/>
            </Attachment>
        </Attachments>
    </Message>
</Contents>
```

What is claimed is:

1. A method for providing a secure transfer of data from a sender to a recipient, comprising the steps of:

transferring said data, including an address of at least one recipient, from said sender to a secure database server located in a network serving said sender;

upon said sender initiating a transfer of said data to said addressed recipient, causing an inquiry to be made as to whether said addressed recipient has an affiliation with said network;

upon a determination of no affiliation, causing said network to dynamically create an account for said addressed recipient, the account including a storage location and an identifier associating said addressed recipient with said storage location;

storing data addressed to said recipient in said storage location;

providing a notification to said addressed recipient of said addressed data being available at said secure database server; and

transferring said addressed data to said addressed recipient upon a request from said addressed recipient.

2. The method of claim 1 wherein said transferred data is constituted as a text message.

3. The method of claim 1 wherein said notification to said addressed recipient is provided via electronic mail message to a non-network address of said addressed recipient.

4. The method of claim 1 including the further steps of:

providing account information in respect to said created account as part of said provided notification.

5. The method of claim 1 wherein said step of transferring said addressed data to said addressed recipient includes the substeps of:

causing said request from said addressed recipient to be directed to said storage location assigned to said addressed recipient, from which said addressed data may be accessed; and

upon said addressed recipient accessing said addressed data at said assigned storage location, causing a notification of that occurrence to be provided to said sender.

6. The method of claim 1 wherein said transferred data is implemented to effect a certified COD system.

7. The method of claim 1 wherein said transferred data is implemented to provide a document escrow arrangement.

8. The method of claim 1 wherein said transferred data is implemented to provide secure, on-line product distribution.

9. The method of claim 1 wherein access to said network for said sender is provided via a wireless terminal.

10. The method of claim 1 wherein said the transferred data is constituted as a facsimile message.

11. The method of claim 1 wherein said transferred data is constituted as confidential financial information.

12. A method for providing a secure transfer of data from a sender to a recipient, comprising the steps of:

transferring said data, including an address of at least one recipient, from said sender to a secure database server located in a network serving said sender;

causing said secure database server to create a storage location for said addressed recipient, when no storage location previously exists for said recipient;

causing said secure database server to place data addressed to said recipient into the storage location assigned to said addressed recipient;

associating said recipient with said storage location via an identifier;

providing a notification to said addressed recipient of said addressed data being available at said secure database server, along with access information corresponding to said identifier for retrieving said addressed data therefrom;

transferring said addressed data to said addressed recipient upon a request from said addressed recipient; and

maintaining said storage location and said identifier for subsequent data transfers.

13. The method of claim 12 wherein said step of transferring said addressed data to said addressed recipient includes the substeps of:

causing said request from said addressed recipient to be directed to said storage location assigned to said addressed recipient, from which said addressed data may be accessed; and

upon said addressed recipient accessing said addressed data at said assigned storage location, causing a notification of that occurrence to be provided to said sender.

14. The method of claim 12 wherein said transferred data is constituted as a text message.

15. The method of claim 12 wherein said notification to said addressed recipient is provided via electronic mail message to a non-network address of said addressed recipient.

16. The method of claim 12 wherein said transferred data is implemented to effect a certified COD system.

17. The method of claim 12 wherein said transferred data is implemented to provide a document escrow arrangement.

18. The method of claim 12 wherein said transferred data is implemented to provide secure, on-line product distribution.

19. The method of claim 12 wherein access to said network for said sender is provided via a wireless terminal.

20. The method of claim 12 wherein said the transferred data is constituted as a facsimile message.

21. The method of claim 12 wherein said transferred data is constituted as confidential financial information.

22. In a network, a method of data transfer comprising the steps of:

upon a sender request to transfer email from the sender to a recipient, determining if a storage location associated with the recipient exists in the network;

if no storage location associated with the recipient exists, automatically creating a unique email account for the recipient, the email account including a storage location and an identifier associating the recipient with the storage location;

storing the email in the storage location; and

maintaining said unique email account for subsequent data transfers.

23. The method of claim 22 further comprising the step of notifying the recipient of the email being available for retrieval and of information concerning the unique account.

24. The method of claim 23 wherein the recipient is notified via a non-network communication path.

* * * * *